Dr. Joseph Teguh Santoso, S.Kom, M.Kom.

BIOMETRIK DAN SISTEM SEKURITI

YAYASAN PRIMA AGUS TEKNIK
UNIVERSITAS SAINS & TEKNOLOGI KOMPUTER
UNIVERSITAS STEKOM

Dr. Joseph Teguh Santoso, S.Kom, M.Kom.

BIOMETRIK DAN SISTEM SEKURITI

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-48-9 (PDF)
9 786238 642489

BIOMETRIK DAN SISTEM SEKURITI

Penulis :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom

ISBN : 978-623-8642-48-9

Editor :
Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : info@stekom.ac.id

DAFTAR ISI

KATA PENGANTAR

Puji syukur kita panjatkan kepada Tuhan Yang Maha Esa, karena atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan buku ini yang berjudul ***"Biometrik Dan Sistem Sekuriti".*** Biometrik, sebagai salah satu teknologi yang semakin berkembang pesat, telah menjadi bagian penting dalam kehidupan sehari-hari, baik dalam aspek keamanan, identifikasi, maupun pengolahan data.

Dalam buku ini, penulis menjelaskan konsep dasar biometrik, jenis-jenisnya, serta penerapannya di berbagai bidang. Harapan penulis, semoga buku ini dapat memberikan pemahaman yang lebih baik tentang pentingnya biometrik dalam era digital saat ini, di mana keamanan dan akurasi identifikasi menjadi sangat krusial.

Dalam masyarakat modern, berbagai aplikasi penting, seperti penyeberangan perbatasan internasional, perdagangan elektronik, dan penyaluran bantuan sosial, sangat membutuhkan sistem pengenalan identitas yang handal. Metode autentikasi tradisional yang bergantung pada kata sandi dan dokumen identitas sering kali tidak memenuhi standar keamanan dan kinerja yang diperlukan, yang mendorong penelitian intensif dalam bidang biometrik. Pengenalan biometrik, atau biometrik sederhana, adalah ilmu yang berfokus pada identifikasi individu melalui atribut fisik atau perilaku, seperti sidik jari, wajah, iris, dan suara.

Sistem biometrik berlandaskan pada prinsip bahwa banyak atribut fisik dan perilaku manusia dapat dihubungkan secara unik dengan individu tertentu. Dengan menggunakan sensor yang dirancang khusus untuk menangkap atribut tersebut, data dapat direpresentasikan dalam format digital dan dibandingkan dengan data yang sebelumnya direkam, sehingga memungkinkan otomatisasi proses pengenalan identitas. Pengenalan biometrik dapat dipandang sebagai masalah pengenalan pola, di mana mesin belajar untuk mengenali fitur-fitur khas dari atribut biometrik individu dan mencocokkannya secara efektif.

Meskipun karakteristik biometrik seperti sidik jari telah lama digunakan dalam bidang forensik, pengembangan sistem biometrik otomatis baru dimulai pada akhir abad ke-20. Namun, penerapan sistem biometrik telah mengalami peningkatan pesat dalam dua dekade terakhir, baik di sektor publik maupun swasta. Perkembangan ini sebagian besar didorong oleh regulasi pemerintah yang mengharuskan penggunaan biometrik untuk memastikan layanan yang aman dan terpercaya.

Dengan demikian, teknologi biometrik memiliki potensi besar untuk mengubah cara kita dikenali dalam berbagai transaksi sehari-hari. Meskipun perkembangan teknologi biometrik berlangsung cepat, studi tentang bidang ini masih terbatas pada kalangan peneliti dan praktisi yang relatif kecil. Hal ini disebabkan oleh dua faktor: pertama, pengenalan biometrik sering dianggap sebagai subjek spesialis yang hanya diajarkan dalam konteks kursus pengenalan pola, visi komputer, atau pemrosesan gambar. Padahal, pengenalan biometrik mencakup banyak aspek penting seperti statistik, desain sensor, rekayasa perangkat lunak, dan faktor manusia. Kedua, pengetahuan tentang biometrik sebagian besar terdapat dalam artikel penelitian dan buku yang ditujukan untuk kalangan akademis, sehingga sulit diakses oleh mereka yang tidak memiliki latar belakang di bidang ini.

Organisasi buku ini dimulai dengan Bab 1 yang memperkenalkan konsep dasar dalam pengenalan biometrik, termasuk cara kerja sistem, terminologi, dan faktor-faktor yang

mempengaruhi desain sistem. Selanjutnya, Bab 2, 3, dan 4 membahas implementasi sistem biometrik berdasarkan karakteristik sidik jari, wajah, dan iris, mengikuti struktur yang sama dengan menjelaskan teknik penginderaan, ekstraksi fitur, dan pencocokan. Bab 2 berfokus pada representasi berbasis detail dan algoritma pencocokan sidik jari, termasuk pengindeksan basis data yang besar dan pengenalan berbasis telapak tangan. Bab 3 membahas deteksi wajah, pendekatan pencocokan foto wajah, serta tantangan seperti variasi pose dan pencahayaan. Sementara Bab 4 mendalami segmentasi iris, pengkodean, dan pencocokan iris menggunakan wavelet Gabor.

Bab 5 menjelaskan teknik pengenalan berdasarkan atribut biometrik tambahan, dan Bab 6 fokus pada sistem multibiometrik yang menggabungkan bukti dari berbagai sumber biometrik. Terakhir, Bab 7 mengulas kerentanan keamanan sistem biometrik dan langkah-langkah untuk mengatasinya, dengan penekanan pada deteksi spoofing dan keamanan template biometrik.

Buku ini diharapkan dapat memberikan wawasan mendalam tentang pengenalan biometrik, membantu pembaca memahami tantangan dan potensi teknologi ini, serta mendorong penelitian dan pengembangan lebih lanjut dalam bidang yang semakin relevan ini. Dengan pemahaman yang lebih baik tentang biometrik, kita dapat memanfaatkan teknologi ini untuk meningkatkan keamanan dan efisiensi dalam berbagai aspek kehidupan sehari-hari.

Semarang, Oktober 2024
Penulis

Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

BAB 1
PENDAHULUAN

Tentang prosedur identifikasi yang memungkinkan ditemukannya kembali nama residivis dengan cara mengandalkan identitasnya sendiri, dan dapat digunakan untuk mengklasifikasi foto-foto di kantor polisi, di kantor polisi umum, di kementerian kehakiman, dll.

Alphonse Bertillon, 1881.

Tentang proses identifikasi yang memungkinkan ditemukannya nama residivis berdasarkan deskripsinya saja, dan yang dapat digunakan dalam konteks pengklasifikasian foto-foto di kantor pusat polisi, di kantor keamanan nasional, di kementerian kehakiman, dll. Kemampuan untuk mengidentifikasi individu secara unik dan mengaitkan atribut pribadi (misalnya, nama, kewarganegaraan, dst.) dengan seorang individu sangat penting bagi struktur masyarakat manusia. Manusia biasanya menggunakan karakteristik tubuh seperti wajah, suara, dan gaya berjalan beserta informasi kontekstual lainnya (misalnya, lokasi dan pakaian) untuk mengenali satu sama lain.

Kumpulan atribut yang dikaitkan dengan seseorang membentuk identitas pribadi mereka. Pada masa-masa awal peradaban, orang-orang hidup dalam komunitas kecil tempat individu-individu dapat dengan mudah mengenali satu sama lain. Namun, ledakan pertumbuhan populasi yang disertai dengan peningkatan mobilitas dalam masyarakat modern telah mengharuskan pengembangan sistem manajemen identitas canggih yang dapat secara efisien merekam, memelihara, dan menghapus identitas pribadi individu.

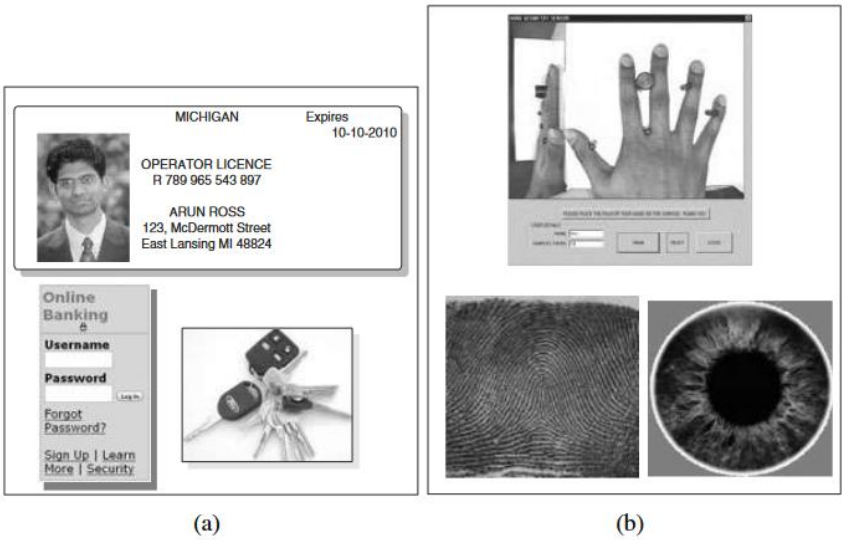
Manajemen identitas memainkan peran penting dalam sejumlah aplikasi. Contoh aplikasi tersebut meliputi pengaturan penyeberangan perbatasan internasional, pembatasan akses fisik ke fasilitas penting seperti pembangkit listrik tenaga nuklir atau bandara, pengendalian akses logis ke sumber daya dan informasi bersama, pelaksanaan transaksi keuangan jarak jauh, atau penyaluran tunjangan kesejahteraan sosial. Perkembangan layanan berbasis web (misalnya, perbankan daring) dan penerapan pusat layanan pelanggan yang terdesentralisasi (misalnya, kartu kredit) telah menimbulkan risiko pencurian identitas. Meningkatnya skala pencurian identitas dan meningkatnya kekhawatiran tentang keamanan nasional telah memperkuat kebutuhan akan sistem manajemen identitas yang andal.

1.1 PENGENALAN PRIBADI

Tugas mendasar dalam manajemen identitas adalah menetapkan hubungan antara individu dan identitas pribadinya. Seseorang harus mampu menentukan identitas seseorang atau memverifikasi klaim identitas seseorang kapan pun diperlukan. Proses ini dikenal sebagai pengenalan pribadi. Seseorang dapat dikenali berdasarkan tiga metode dasar berikut (lihat Gambar 1.1): (a) apa yang diketahuinya, (b) apa yang dimilikinya secara ekstrinsik, dan (c) siapa dirinya secara intrinsik. Sementara metode pertama bergantung pada fakta bahwa individu tersebut memiliki pengetahuan eksklusif tentang beberapa informasi rahasia (misalnya, kata sandi, nomor identifikasi pribadi, atau kunci kriptografi),

metode kedua mengasumsikan bahwa orang tersebut memiliki kepemilikan eksklusif atas token ekstrinsik (misalnya, kartu identitas, SIM, paspor, kunci fisik, atau perangkat pribadi seperti ponsel). Metode ketiga menetapkan identitas seseorang berdasarkan ciri fisik atau perilaku bawaannya dan dikenal sebagai pengenalan biometrik. Secara formal, pengenalan biometrik dapat didefinisikan sebagai ilmu untuk menetapkan identitas seseorang berdasarkan karakteristik fisik dan/atau perilaku orang tersebut, baik secara otomatis penuh maupun semi-otomatis.

Pengenalan orang berbasis pengetahuan dan berbasis token bergantung pada representasi identitas pengganti seperti kata sandi atau kartu identitas, yang dapat dengan mudah dilupakan/hilang, ditebak/dicuri, atau dibagikan. Selain itu, mereka tidak dapat menyediakan fungsi manajemen identitas yang penting seperti tidak dapat disangkal dan mendeteksi beberapa pendaftaran oleh orang yang sama dengan identitas yang berbeda. Misalnya, individu dapat dengan mudah menyangkal (menolak) penggunaan suatu layanan dengan mengklaim bahwa kata sandi mereka telah dicuri atau ditebak. Individu juga dapat menyembunyikan identitas asli mereka dengan menunjukkan dokumen identifikasi palsu atau duplikat. Selain itu, mekanisme tradisional seperti kata sandi dan token tidak memberikan bukti yang kuat untuk pengenalan orang pasca-peristiwa, seperti identifikasi tersangka di tempat kejadian perkara. Oleh karena itu, semakin jelas bahwa mekanisme berbasis pengetahuan dan berbasis token saja tidak cukup untuk manajemen identitas yang andal.



Gambar 1.1 Tiga pendekatan dasar untuk pengenalan orang.

(a) Skema tradisional menggunakan kata sandi ("apa yang Anda ingat") dan kartu identitas atau kunci ("apa yang Anda miliki secara ekstrinsik") untuk memvalidasi individu dan memastikan bahwa sumber daya sistem hanya diakses oleh individu yang terdaftar secara sah,
(b) dengan munculnya biometrik, kini memungkinkan untuk menetapkan identitas berdasarkan "siapa Anda secara intrinsik".

Pengenalan biometrik, atau biometrik, menawarkan solusi alami dan lebih andal untuk masalah pengenalan orang. Karena pengenal biometrik melekat pada individu, lebih

sulit untuk memanipulasi, berbagi, atau melupakan ciri-ciri ini. Oleh karena itu, ciri-ciri biometrik merupakan hubungan yang kuat dan cukup permanen antara seseorang dan identitasnya. Setiap orang yang menunjukkan pengenal biometriknya ke sistem biometrik untuk tujuan dikenali dapat disebut sebagai pengguna sistem.

Karena sistem biometrik mengharuskan pengguna untuk hadir pada saat autentikasi, sistem ini juga dapat mencegah pengguna membuat klaim penolakan palsu. Selain itu, hanya biometrik yang dapat menetapkan apakah individu tertentu sudah dikenal oleh sistem manajemen identitas, meskipun individu tersebut mungkin menyangkalnya. Hal ini sangat penting dalam aplikasi seperti pencairan kesejahteraan, di mana seorang penipu dapat mencoba mengklaim beberapa manfaat (misalnya, double dipping). Karena alasan-alasan di atas, pengenalan biometrik semakin banyak diadopsi dalam sejumlah aplikasi manajemen identitas pemerintah dan sipil, baik untuk menggantikan atau melengkapi mekanisme berbasis pengetahuan dan berbasis token yang ada.

1.2 SISTEM BIOMETRIK

Sistem biometrik mengukur satu atau lebih karakteristik fisik atau perilaku (lihat Gambar 1.2), termasuk sidik jari, telapak tangan, wajah, iris, retina, telinga, suara, tanda tangan, gaya berjalan, urat tangan, bau, atau informasi DNA seseorang untuk menentukan atau memverifikasi identitasnya. Karakteristik ini disebut dengan istilah yang berbeda seperti sifat, indikator, pengenal, atau modalitas. Dalam bab ini, berbagai blok penyusun sistem biometrik generik dan isu-isu yang terlibat dalam desain, implementasi, dan evaluasi sistem tersebut akan dibahas. Rincian tentang implementasi sistem biometrik berdasarkan sifat biometrik tertentu akan dibahas dalam bab-bab berikutnya.

Tahap pendaftaran dan pengenalan

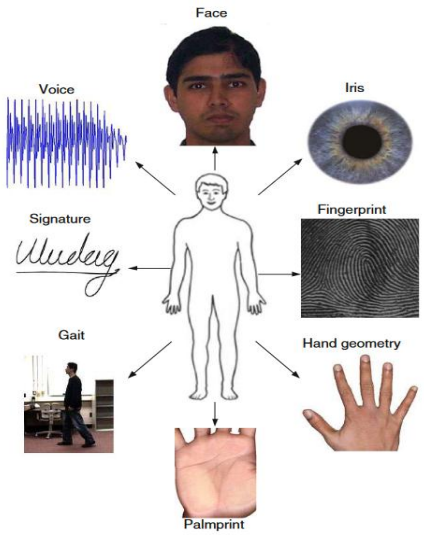
Bagaimana sistem biometrik mengidentifikasi pengguna berdasarkan ciri fisik dan/atau perilakunya? Proses ini terdiri dari dua tahap utama, yaitu pendaftaran dan pengenalan (lihat Gambar 1.2). Selama tahap pendaftaran, data biometrik diperoleh dari individu dan disimpan dalam basis data bersama dengan identitas orang tersebut. Biasanya, data biometrik yang diperoleh diproses untuk mengekstraksi fitur yang menonjol dan khas.

Dalam banyak kasus, hanya kumpulan fitur yang diekstraksi yang disimpan, sedangkan data biometrik mentah dibuang. Selama tahap pengenalan, data biometrik diperoleh kembali dari individu dan dibandingkan dengan data yang disimpan untuk menentukan identitas pengguna. Dengan demikian, sistem biometrik pada dasarnya adalah sistem pengenalan pola (atau pencocokan pola) yang terdiri dari empat blok penyusun dasar, yaitu, (a) sensor, (b) ekstraktor fitur, (c) basis data, dan (d) pencocok seperti yang ditunjukkan pada Gambar 1.3. Keempat modul ini sekarang akan dibahas secara bergantian.

Modul sensor

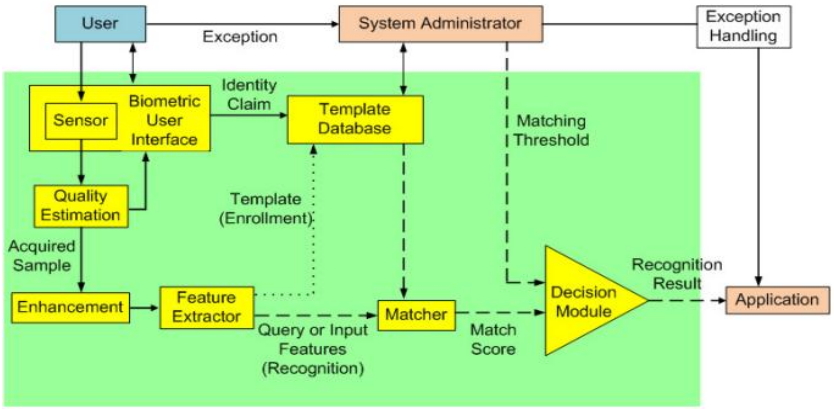
Antarmuka pengguna yang sesuai yang menyertakan sensor atau pembaca biometrik diperlukan untuk mengukur atau merekam data biometrik mentah pengguna. Misalnya, sensor sidik jari optik dapat digunakan untuk mengambil gambar pola tonjolan gesekan di ujung jari. Desain antarmuka pengguna (atau manusia-mesin) yang baik sangat penting

untuk keberhasilan penerapan sistem biometrik. Antarmuka yang intuitif, ergonomis, dan mudah digunakan dapat memfasilitasi pembiasaan pengguna yang cepat dan memungkinkan perolehan sampel biometrik berkualitas baik dari pengguna.



Gambar 1.2 Contoh ciri tubuh yang telah digunakan untuk pengenalan biometrik.

Ciri fisik meliputi wajah, sidik jari, iris, telapak tangan, geometri tangan, suara, dan bentuk telinga, sementara gaya berjalan, tanda tangan, dan dinamika penekanan tombol adalah beberapa karakteristik perilaku. Perbedaan antara ciri fisik dan karakteristik perilaku sebenarnya tidak terlalu penting. Ini karena data biometrik yang diambil dari seorang individu biasanya merupakan manifestasi dari aspek fisik dan perilaku orang tersebut. Misalnya, sementara sidik jari adalah ciri fisik, gambar sidik jari yang diperoleh dari seseorang juga bergantung pada bagaimana ia berinteraksi dengan sensor, yaitu, perilaku pengguna. Demikian pula, sementara gaya berjalan mungkin merupakan ciri perilaku, itu sampai batas tertentu ditentukan oleh karakteristik fisik tubuh manusia.



Gambar 1.3 Blok penyusun dasar sistem biometrik generik.

Kualitas sampel biometrik mentah juga bergantung pada karakteristik sensor yang digunakan. Untuk sebagian besar modalitas biometrik, data biometrik mentah berbentuk

gambar dua dimensi (misalnya, sidik jari, wajah, iris, dll.). Pengecualiannya meliputi suara (sinyal amplitudo 1 dimensi), tanda tangan daring (tekanan pena, posisi, dan kecepatan), bau, dan DNA (berbasis kimia). Untuk data berbasis gambar, faktor-faktor seperti resolusi, frame rate, dan sensitivitas kamera memainkan peran penting dalam menentukan kualitas gambar.

Gambar 1.4 menunjukkan gambar sidik jari pada dua resolusi berbeda yang diperoleh menggunakan sensor sidik jari yang berbeda. Seseorang mungkin juga perlu mempertimbangkan karakteristik demografis populasi target seperti usia dan jenis kelamin, dan masalah budaya lainnya (misalnya, beberapa pengguna mungkin enggan menyentuh permukaan sensor) saat merancang modul sensor. Lebih jauh, faktor-faktor seperti biaya, ukuran, dan daya tahan juga memengaruhi desain sensor.

Gambar 1.4 Sidik jari dipindai pada (a) 1000 titik per inci (ppi) dan (b) 500 titik per inci menggunakan sensor sidik jari yang berbeda.

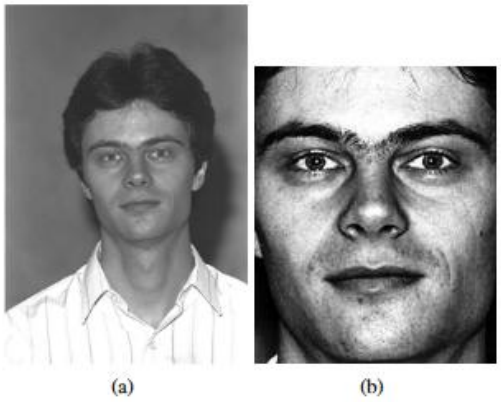
Modul ekstraksi fitur

Biasanya, data biometrik mentah dari sensor mengalami operasi pra-pemrosesan sebelum fitur diekstraksi darinya. Tiga langkah pra-pemrosesan yang umum digunakan adalah (a) penilaian kualitas, (b) segmentasi, dan (c) peningkatan. Pertama, kualitas sampel biometrik yang diperoleh perlu diakses untuk menentukan kesesuaiannya untuk pemrosesan lebih lanjut. Jika data mentah tidak memiliki kualitas yang memadai, ada dua pilihan. Seseorang dapat mencoba untuk memperoleh kembali data dari pengguna atau memicu pengecualian (alarm kegagalan) yang memberi tahu administrator sistem untuk mengaktifkan prosedur alternatif yang sesuai (biasanya melibatkan beberapa bentuk intervensi manual oleh operator sistem).

Langkah pra-pemrosesan berikutnya dikenal sebagai segmentasi, yang tujuannya adalah untuk memisahkan data biometrik yang diperlukan dari kebisingan latar belakang. Mendeteksi wajah dalam gambar yang berantakan adalah contoh segmentasi yang baik. Terakhir, data biometrik tersegmentasi dikenakan algoritma peningkatan kualitas sinyal untuk meningkatkan kualitasnya dan mengurangi noise lebih lanjut. Dalam kasus data gambar, algoritma peningkatan seperti penghalusan atau pemerataan histogram dapat diterapkan untuk meminimalkan noise yang disebabkan oleh kamera atau variasi

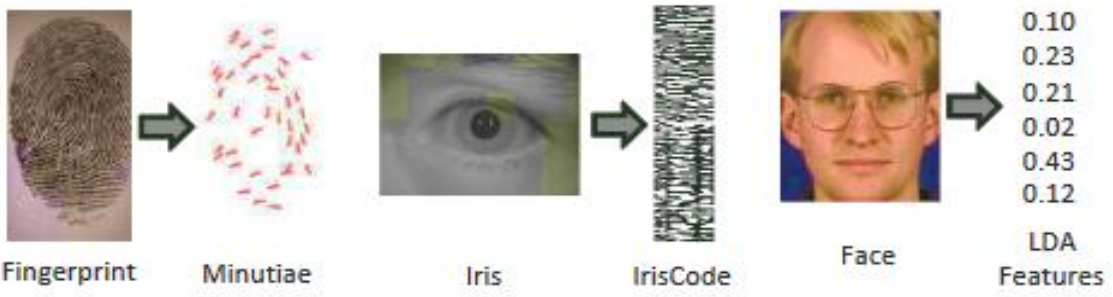
pencahayaan. Gambar 1.5 menunjukkan gambar wajah yang diperoleh setelah segmentasi dan peningkatan kualitas berdasarkan pemerataan histogram. Dalam beberapa kasus, langkah pra-pemrosesan di atas mungkin tidak dapat dipisahkan dari langkah ekstraksi fitur yang sebenarnya. Misalnya, penilaian kualitas itu sendiri mungkin memerlukan ekstraksi beberapa fitur dari data biometrik yang diperoleh.

Detail rumit dari sidik jari seperti lokasi pori-pori keringat dapat lebih mudah diamati pada gambar sidik jari beresolusi tinggi yang ditunjukkan pada (a) dibandingkan dengan gambar beresolusi rendah pada (b). Ekstraksi fitur mengacu pada proses menghasilkan representasi digital yang ringkas tetapi ekspresif dari ciri biometrik yang mendasarinya, yang disebut templat. Templat diharapkan hanya berisi informasi diskriminatif yang menonjol yang penting untuk mengenali orang tersebut. Misalnya, posisi dan orientasi titik-titik minutia (lokasi di mana tonjolan gesekan pada pola sidik jari menunjukkan beberapa anomali) diyakini unik untuk setiap jari. Oleh karena itu, mendeteksi titik-titik kecil pada citra sidik jari merupakan langkah ekstraksi fitur utama dalam sebagian besar sistem biometrik berbasis sidik jari. Gambar 1.6 menunjukkan fitur-fitur yang umum diekstraksi yang digunakan untuk merepresentasikan citra sidik jari, iris, dan wajah.



Gambar 1.5 Segmentasi dan peningkatan wajah.

(a) Citra wajah seseorang sebagaimana yang ditangkap oleh kamera dan (b) citra wajah yang diproses yang diperoleh setelah segmentasi (penghapusan latar belakang dan daerah non-wajah lainnya seperti rambut dan daerah di bawah dagu) dan peningkatan kontras berdasarkan pemerataan histogram.



Gambar 1.6 Fitur umum yang diekstrak dari sidik jari, iris, dan wajah.

Sidik jari umumnya direpresentasikan sebagai sekumpulan titik yang menggambarkan hal-hal kecil; iris direpresentasikan sebagai vektor biner yang menggambarkan respons biner dari gambar masukan terhadap filter Gabor; wajah umumnya direpresentasikan sebagai vektor bilangan riil yang menggambarkan, misalnya, koefisien Analisis Diskriminan Linier (LDA). Selama pendaftaran, templat disimpan baik dalam basis data pusat sistem biometrik atau direkam pada token (misalnya, kartu pintar) yang dikeluarkan untuk individu berdasarkan sifat aplikasi.

Pada saat pengenalan, templat diambil dari basis data, dan dicocokkan dengan set fitur yang diekstrak dari sampel biometrik baru yang diperoleh dari pengguna. Set fitur baru yang diperoleh dalam fase pengenalan ini biasanya disebut sebagai kueri atau masukan. Dalam banyak sistem biometrik berbasis gambar (misalnya, wajah atau sidik jari), gambar biometrik mentah juga dapat disimpan dalam basis data bersama dengan templat selama pendaftaran.

Gambar tersebut sering dikenal sebagai gambar galeri, gambar referensi, gambar tersimpan, atau gambar pendaftaran. Gambar yang diperoleh selama pengenalan dikenal sebagai gambar probe, gambar kueri, atau gambar input. Templat pengguna dapat diekstraksi dari satu sampel biometrik, atau dibuat dengan memproses beberapa sampel yang diperoleh selama pendaftaran. Dengan demikian, templat minutiae dari jari dapat diekstraksi setelah membuat mosaik (menggabungkan) beberapa kesan dari jari yang sama.

Beberapa sistem menyimpan beberapa templat untuk memperhitungkan variasi besar yang dapat diamati dalam data biometrik pengguna. Sistem pengenalan wajah, misalnya, dapat menyimpan beberapa templat individu, dengan setiap templat sesuai dengan pose wajah yang berbeda sehubungan dengan kamera. Modul basis data Basis data sistem biometrik bertindak sebagai gudang informasi biometrik. Selama proses pendaftaran, set fitur yang diekstrak dari sampel biometrik mentah (yaitu, templat) disimpan dalam basis data bersama dengan beberapa informasi identitas pribadi (seperti nama, Nomor Identifikasi Pribadi (PIN), alamat, dll.) yang mencirikan pengguna.

Salah satu keputusan utama dalam desain sistem biometrik adalah apakah akan menggunakan basis data terpusat atau yang terdesentralisasi. Menyimpan semua templat dalam basis data pusat mungkin bermanfaat dari perspektif keamanan sistem, karena data dapat diamankan melalui isolasi fisik dan dengan memiliki mekanisme kontrol akses yang ketat. Di sisi lain, kompromi basis data pusat akan memiliki implikasi yang jauh lebih besar daripada kompromi salah satu situs dalam basis data terdesentralisasi. Ini karena individu jahat (administrator atau peretas yang korup) dapat menyalahgunakan informasi biometrik yang disimpan dalam basis data untuk membahayakan privasi pengguna yang tidak bersalah.

Modul pencocokan

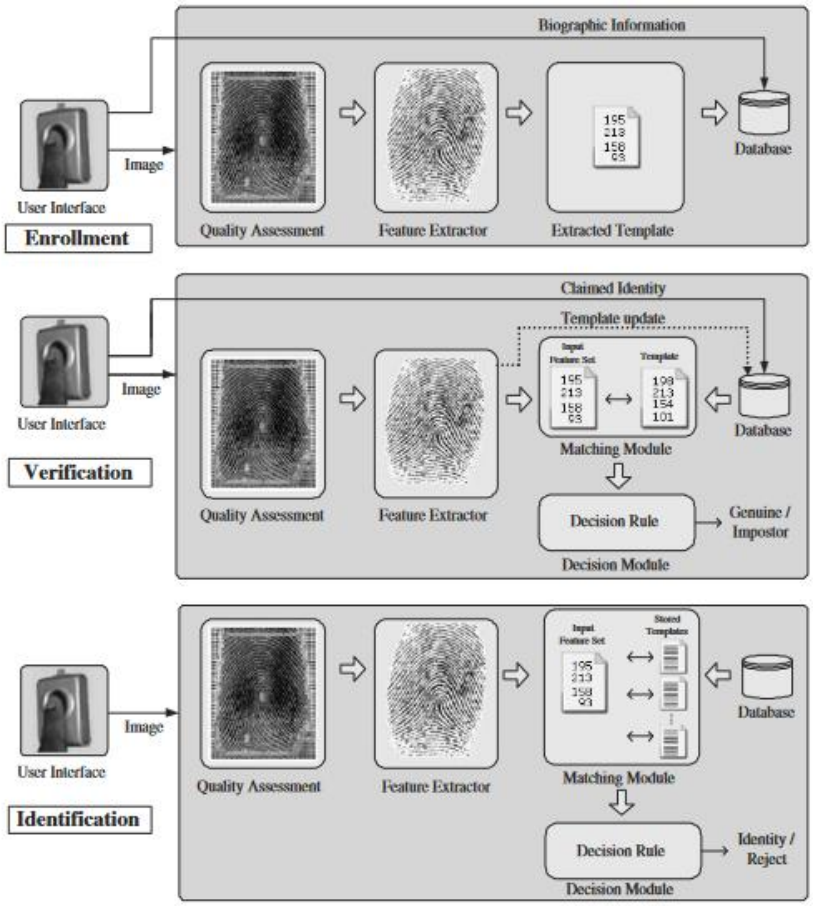
Tujuan pencocok biometrik adalah membandingkan fitur kueri dengan templat yang tersimpan untuk menghasilkan skor pencocokan. Skor pencocokan adalah ukuran kesamaan antara templat dan kueri. Oleh karena itu, skor pencocokan yang lebih besar menunjukkan kesamaan yang lebih besar antara templat dan kueri. Jika pencocok mengukur perbedaan

(bukan kesamaan) antara dua set fitur, skor tersebut disebut sebagai skor jarak. Skor jarak yang lebih kecil menunjukkan kesamaan yang lebih besar.

Dalam sistem biometrik berbasis sidik jari, jumlah detail pencocokan antara set fitur masukan dan templat dapat dianggap sebagai tingkat kesamaan (skor pencocokan). Skor pencocokan juga dapat dimoderasi berdasarkan kualitas data biometrik yang disajikan. Modul pencocok juga merangkum modul pengambilan keputusan, di mana skor pencocokan digunakan untuk memvalidasi identitas yang diklaim atau memberikan peringkat identitas yang terdaftar untuk mengidentifikasi seseorang.

1.3 FUNGSIONALITAS BIOMETRIK

Sistem biometrik dapat menyediakan dua jenis fungsionalitas manajemen identitas, yaitu verifikasi dan identifikasi. Dalam buku ini, istilah umum pengenalan akan digunakan ketika kita tidak ingin membedakan antara fungsionalitas verifikasi dan identifikasi. Selain itu, istilah autentikasi akan digunakan sebagai sinonim untuk verifikasi. Gambar 1.7 menunjukkan fase pendaftaran dan pengenalan sistem biometrik yang beroperasi dalam mode verifikasi dan identifikasi.



Gambar 1.7 Tahapan pendaftaran dan pengenalan sistem biometrik yang beroperasi dalam mode verifikasi dan identifikasi. Garis putus-putus dalam modul verifikasi merupakan operasi opsional untuk memperbarui templat pengguna tertentu.

Verifikasi

Dalam verifikasi, pengguna mengklaim identitas dan sistem memverifikasi apakah klaim tersebut asli, yaitu, sistem menjawab pertanyaan "Apakah Anda seperti yang Anda katakan?". Dalam skenario ini, kueri hanya dibandingkan dengan templat yang sesuai dengan identitas yang diklaim (kecocokan satu lawan satu). Klaim identitas biasanya dilakukan melalui penggunaan Nomor Identifikasi Pribadi (PIN), nama pengguna, atau token (misalnya, kartu pintar).

Jika masukan pengguna dan templat identitas yang diklaim memiliki tingkat kesamaan yang tinggi, maka klaim tersebut diterima sebagai "asli". Jika tidak, klaim tersebut ditolak dan pengguna dianggap sebagai "penipu". Dalam literatur biometrik, istilah "klien" atau "asli" terkadang digunakan sebagai pengganti istilah "asli". Verifikasi biasanya digunakan dalam aplikasi yang tujuannya adalah untuk mencegah orang yang tidak berwenang menggunakan layanan.

Secara formal, verifikasi dapat diajukan sebagai masalah klasifikasi dua kategori berikut: dengan identitas yang diklaim I dan set fitur kueri $\mathbf{x}^A$, kita perlu memutuskan apakah $(I, \mathbf{x}^A)$ termasuk dalam kelas “asli” atau “penipu”. Biarkan $\mathbf{x}^A$, kita perlu memutuskan apakah $\mathbf{x}_I^E$ menjadi templat tersimpan yang sesuai dengan identitas I. Biasanya, $\mathbf{x}^A$ dibandingkan dengan $\mathbf{x}_I^E$ dan skor kecocokan s, yang mengukur kesamaan antara $\mathbf{x}^A$ dan $\mathbf{x}_I^E$, dihitung. Aturan keputusan diberikan oleh

$$(I, x^A)\epsilon \begin{cases} asli, jika\ s \geq \eta, \\ penipu, jika\ s < \eta, \end{cases} \tag{1.1}$$

di mana η adalah ambang batas yang telah ditetapkan sebelumnya. Jika skor jarak digunakan sebagai pengganti skor kesamaan atau kecocokan, ketidaksetaraan dalam aturan keputusan yang ditunjukkan dalam persamaan (1.1) harus dibalik. Ketika klaim identitas dianggap "asli", pengguna diizinkan untuk mengakses layanan yang disediakan oleh sistem.

Identifikasi

Fungsionalitas identifikasi dapat diklasifikasikan lebih lanjut menjadi identifikasi positif dan negatif. Dalam identifikasi positif, pengguna mencoba mengidentifikasi dirinya secara positif ke sistem tanpa secara eksplisit mengklaim identitas. Sistem identifikasi positif menjawab pertanyaan "Apakah Anda seseorang yang dikenal oleh sistem?" dengan menentukan identitas pengguna dari serangkaian identitas yang diketahui.

Sebaliknya, pengguna dalam aplikasi identifikasi negatif dianggap menyembunyikan identitas aslinya (baik secara eksplisit maupun implisit) dari sistem. Identifikasi negatif juga dikenal sebagai penyaringan dan tujuan dari sistem tersebut adalah untuk mengetahui “Apakah Anda orang yang Anda katakan bukan Anda?”. Tujuan dari identifikasi negatif adalah untuk mencegah satu orang menggunakan beberapa identitas.

Oleh karena itu, penyaringan dapat digunakan untuk mencegah penerbitan beberapa catatan kredensial (misalnya, SIM, paspor) yang diberikan kepada orang yang sama atau untuk mencegah seseorang mengklaim beberapa tunjangan dengan nama yang berbeda

(masalah yang umum ditemui dalam aplikasi pencairan kesejahteraan). Penyaringan juga sering digunakan di bandara untuk memverifikasi apakah identitas penumpang cocok dengan seseorang dalam "daftar pantauan".

Dalam identifikasi positif dan negatif, masukan biometrik pengguna dibandingkan dengan templat semua orang yang terdaftar dalam basis data dan sistem mengeluarkan identitas orang yang templatnya memiliki tingkat kesamaan tertinggi dengan masukan pengguna atau keputusan yang menunjukkan bahwa pengguna yang menyajikan masukan tersebut bukan pengguna terdaftar. Secara formal, masalah identifikasi dapat dinyatakan sebagai berikut: diberikan set fitur kueri $\mathbf{x}^A$, kita perlu memutuskan identitas I pengguna, di mana $I \in \{I_1, I_2, \dots, I_N, I_{N+1}\}$. Di sini, I_1, I_2, I_N sesuai dengan identitas pengguna N yang terdaftar dalam sistem dan I_{N+1} menunjukkan kasus di mana tidak ada identitas yang cocok dapat ditentukan untuk kueri yang diberikan. Jika $\mathbf{x}_{In}^E$ adalah templat tersimpan yang sesuai dengan identitas I_n dan s_n adalah skor kecocokan antara $\mathbf{x}^A$ dan $\mathbf{x}_{In}^E$, untuk $n = 1, 2, \cdots, N$, aturan keputusan untuk identifikasi adalah,

$$\mathbf{x}^A \epsilon \begin{cases} I_{n_0}, if\ n_0 = \arg\max s_n \text{ dan } s_{n_0} \geq \eta \\ I_{N+1}, lainnya, \end{cases} \tag{1.2}$$

di mana η adalah ambang batas yang telah ditentukan sebelumnya. Aturan keputusan di atas umumnya dikenal sebagai identifikasi set terbuka, karena memungkinkan untuk mengembalikan hasil yang menunjukkan bahwa pengguna yang menunjukkan sifat biometriknya tidak termasuk di antara N pengguna yang terdaftar. Hampir semua sistem identifikasi biometrik praktis (termasuk sistem penyaringan) menggunakan identifikasi set terbuka. Dimungkinkan juga untuk memaksa sistem untuk mengembalikan satu di antara N identitas yang terdaftar, terlepas dari nilai s_{n_0}. Skenario seperti itu disebut identifikasi set tertutup.

Dalam beberapa sistem identifikasi biometrik praktis (misalnya, pencocokan sidik jari laten), identifikasi bersifat semi-otomatis. Sistem biometrik semi-otomatis mengeluarkan identitas dari t kecocokan teratas $(1 < t \ll N)$ dan seorang ahli manusia secara manual menentukan identitas (di antara t identitas yang dipilih) yang paling cocok dengan kueri yang diberikan.

Nilai t dapat ditentukan berdasarkan ketersediaan dan hasil kerja pakar manusia. Terhadap basis data besar seperti Sistem Identifikasi Sidik Jari Otomatis Terpadu (IAFIS) milik FBI, yang memiliki sekitar 60 juta pengguna terdaftar, nilai t yang umum dapat berkisar antara 20 hingga 50. Pendekatan lain adalah mengembalikan semua identitas yang skor kecocokannya melebihi ambang batas (η) dalam persamaan (1.2). Karena jumlah pengguna terdaftar dalam basis data bisa sangat besar (misalnya, FBI-IAFIS), tugas identifikasi jauh lebih menantang daripada verifikasi.

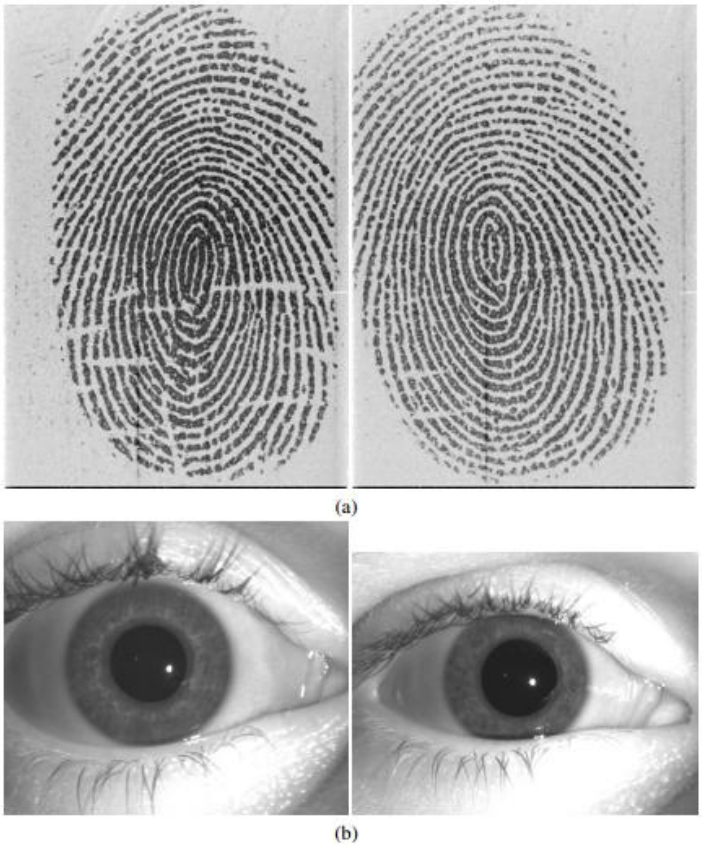
1.4 KESALAHAN SISTEM BIOMETRIK

Ilmu pengenalan biometrik didasarkan pada dua premis mendasar, yaitu keunikan dan keawetan ciri biometrik yang mendasarinya. Pengenal biometrik dikatakan unik hanya jika dua orang di dunia dapat dibedakan berdasarkan pengenal yang diberikan. Ciri biometrik bersifat permanen jika tidak berubah selama hidup seseorang. Namun, kedua premis ini jarang berlaku dalam sistem biometrik praktis. Hal ini terutama disebabkan oleh dua alasan.

Pertama, ciri fisik itu sendiri mungkin tidak unik. Misalnya, ketika sistem pengenalan sidik jari mulai populer pada awal abad ke-20, laporan pers mengklaim bahwa sidik jari benar-benar unik. “Hanya sekali selama keberadaan tata surya kita, dua manusia akan lahir dengan tanda jari yang sama” - Judul berita Harper, 1910.

“Dua sidik jari yang sama hanya akan ditemukan sekali setiap 1048 tahun” –
Scientific American, 1911.

Klaim semacam itu diterima dari waktu ke waktu, bukan karena bukti ilmiah yang kuat yang mendukungnya, tetapi lebih karena kurangnya kontradiksi dan pengulangan yang tiada henti. Dalam dua dekade terakhir, klaim tentang keunikan sidik jari telah ditentang oleh komunitas ilmiah dan hukum. Demikian pula, keunikan atau individualitas modalitas biometrik lainnya belum ditetapkan dengan jelas.


(a)

(b)

Gambar 1.8 Biometrik pasangan kembar.

(a) Sidik jari telunjuk kanan pasangan kembar; (b) Mata kanan pasangan kembar; (c) Citra wajah pasangan kembar.

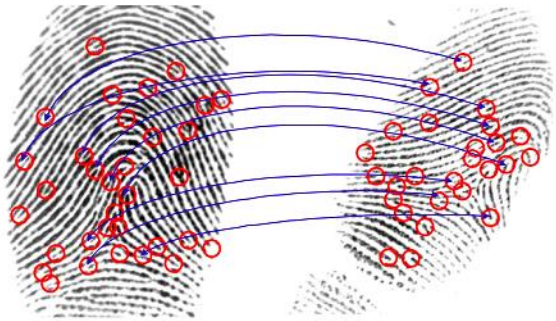
Kesamaan genetik antara individu yang terkait (misalnya, saudara kembar, ayah dan anak) juga dapat berkontribusi pada kurangnya keunikan beberapa ciri biometrik. Misalnya, penampilan wajah saudara kembar identik hampir sama. Modalitas seperti DNA, di mana konstitusi genetik individu sangat menentukan karakteristik biometrik mereka disebut sebagai faktor/fitur genotipik. Sebaliknya, modalitas yang karakteristiknya ditentukan oleh sumber keacakan lain di alam (misalnya, sidik jari) disebut sebagai faktor/fitur fenotipik. Gambar 1.8 menunjukkan gambar sidik jari, wajah, dan iris yang diperoleh dari saudara kembar identik.

Lebih jauh, gagasan bahwa ciri-ciri biometrik bersifat permanen juga bukan fakta ilmiah yang mapan. Efek pertumbuhan tubuh (terutama selama masa kanak-kanak dan remaja) pada pengenal biometrik umum seperti wajah, sidik jari, atau iris, belum dipelajari secara rinci. Bahkan dengan mengesampingkan kemungkinan perubahan alami pada ciri-ciri fisik, sistem biometrik praktis menghadapi masalah yang jauh lebih menantang. Sistem biometrik hanya bergantung pada pengukuran digital karakteristik tubuh, dan bukan ciri fisik yang sebenarnya.

Proses pengukuran (penginderaan) ini menghasilkan variasi dalam sampel ciri biometrik yang sama dari pengguna yang diperoleh selama kurun waktu tertentu. Akibatnya, rangkaian fitur yang diperoleh dari sampel yang berbeda dari ciri biometrik yang sama dari pengguna jarang identik. Variabilitas yang diamati dalam rangkaian fitur biometrik individu dikenal sebagai variasi intra-pengguna atau variasi intra-kelas.

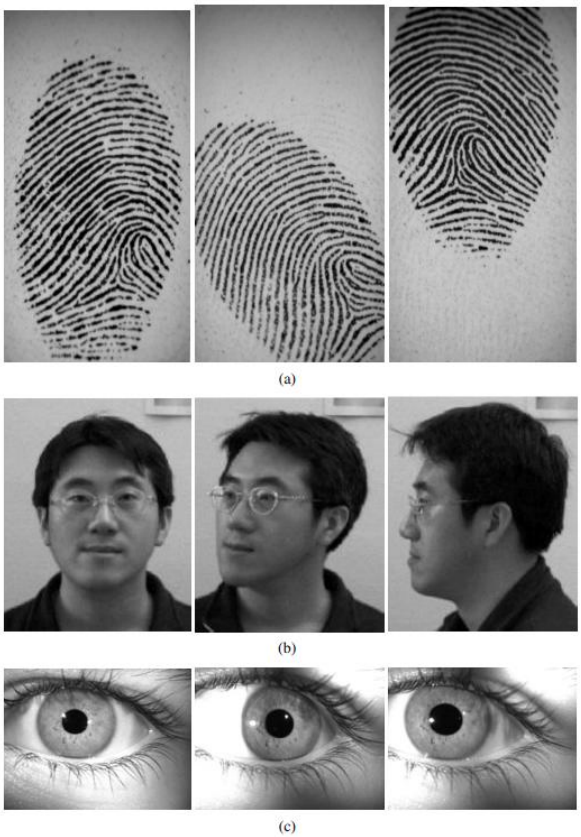
Variabilitas ini mungkin disebabkan oleh alasan seperti kondisi penginderaan yang tidak sempurna (misalnya, sidik jari yang berisik karena kerusakan sensor), perubahan karakteristik biometrik pengguna (misalnya, penyakit pernapasan yang memengaruhi pengenalan pembicara), perubahan kondisi sekitar (misalnya, tingkat pencahayaan yang tidak konsisten dalam aplikasi pengenalan wajah), dan variasi dalam interaksi pengguna dengan sensor (misalnya, iris yang tertutup atau sidik jari sebagian). Sebagai ilustrasi, perhatikan dua kesan dari jari yang sama yang diperoleh pada hari yang berbeda yang ditunjukkan pada Gambar 1.9. Kesan-kesan ini berbeda dalam hal distorsi geometrik dan jumlah tumpang tindih yang disebabkan oleh faktor-faktor seperti penempatan jari pada

sensor, tekanan jari yang diberikan, kondisi kulit, dan kesalahan ekstraksi fitur. Demikian pula, Gambar 1.10 menunjukkan variasi intra-pengguna pada citra wajah seseorang karena perubahan pose dan atribut lain seperti rambut wajah.



Gambar 1.9 Ilustrasi variabilitas intra-pengguna pada sidik jari.

Dua cetakan berbeda dari sidik jari yang sama yang diperoleh pada hari yang berbeda ditunjukkan dengan titik-titik minutia yang ditandai di atasnya. Karena perbedaan penempatan jari dan distorsi yang disebabkan oleh variasi tekanan jari, jumlah dan lokasi minutia pada kedua gambar berbeda (masing-masing 33 dan 26 pada gambar kiri dan kanan). Jumlah minutia yang sesuai/cocok pada kedua gambar hanya 16. Beberapa dari korespondensi ini telah ditunjukkan pada gambar. Konsep titik-titik minutia akan dijelaskan pada bab berikutnya.



Gambar 1.10 Variasi intra-pengguna.

(a) Variasi sidik jari orang yang sama akibat perbedaan posisi dan orientasi sidik jari, (b) variasi citra wajah orang yang sama akibat perubahan pose, dan (c) variasi citra iris akibat perbedaan dilatasi dan arah pandangan.

Variasi intra-pengguna bahkan lebih menonjol dalam sifat-sifat perilaku karena susunan psikologis individu yang bervariasi dapat mengakibatkan karakteristik perilaku yang sangat berbeda pada waktu yang berbeda. Misalnya, tergantung pada tingkat stres seseorang, sampel suara yang ditunjukkan oleh orang tersebut pada saat autentikasi mungkin sangat berbeda dari templat yang terdaftar. Demikian pula, gaya berjalan dan tanda tangan orang yang mabuk mungkin berubah secara substansial.

Mengingat variabilitas dalam ciri biometrik yang diperoleh, adalah suatu hal yang dibuat-buat untuk mengharapkan kecocokan yang sempurna antara dua set fitur biometrik, bahkan jika keduanya berasal dari orang yang sama. Bahkan, jika dua set fitur memang identik, itu mungkin merupakan indikasi kuat bahwa data biometrik sebenarnya berasal dari musuh yang memutar ulang data yang direkam pada waktu sebelumnya. Oleh karena itu, ada perbedaan mendasar antara sistem autentikasi berbasis kata sandi dan sistem biometrik.

Dalam sistem berbasis kata sandi, kecocokan sempurna antara dua string alfanumerik diperlukan untuk memvalidasi identitas pengguna. Di sisi lain, sistem biometrik sebagian besar memutuskan identitas seseorang berdasarkan kecocokan dekat antara templat dan kueri, di mana kekuatan kecocokan (atau tingkat kesamaan) diwakili oleh skor kecocokan.

Seperangkat fitur biometrik yang ideal harus menunjukkan kesamaan antarpengguna yang kecil dan variasi intrapengguna yang kecil. Dalam praktiknya, kedua kondisi ini mungkin tidak sepenuhnya terpenuhi baik karena keterbatasan informasi yang melekat (kurangnya keunikan) dalam sifat biometrik yang mendasarinya atau karena keterbatasan representasi (masalah dalam ekstraksi fitur). Sistem ekstraksi fitur praktis, yang biasanya didasarkan pada model data biometrik yang sederhana, gagal menangkap kekayaan informasi dalam input biometrik yang realistis yang mengakibatkan penyertaan fitur yang berlebihan atau palsu, dan pengecualian fitur yang menonjol.

Karena kesamaan antarpengguna yang besar dan variasi intrapengguna yang besar, sistem biometrik dapat membuat dua jenis kesalahan, yaitu, ketidakcocokan palsu dan kecocokan palsu. Bila variasi intra-pengguna besar, dua sampel dengan ciri biometrik yang sama dari seorang individu (sampel pasangan) mungkin tidak dikenali sebagai kecocokan, dan ini menyebabkan kesalahan ketidakcocokan palsu. Kecocokan palsu terjadi bila dua sampel dari individu yang berbeda (sampel non-pasangan) dikenali secara keliru sebagai kecocokan karena kesamaan antar-pengguna yang besar.

Ukuran kinerja

Ukuran dasar keakuratan sistem biometrik adalah *False Non-Match Rate* (FNMR) dan *False Match Rate* (FMR). FNMR merujuk pada probabilitas yang diharapkan bahwa dua sampel pasangan (sampel dengan ciri biometrik yang sama yang diperoleh dari pengguna yang sama) akan dinyatakan secara keliru sebagai ketidakcocokan. FMR adalah probabilitas

yang diharapkan bahwa dua sampel non-pasangan akan dikenali secara keliru sebagai kecocokan.

False Non-Match Rate sebesar 5% menunjukkan bahwa rata-rata, 5 dari 100 upaya autentikasi oleh pengguna asli tidak akan berhasil. Sebagian besar kesalahan ketidakcocokan palsu biasanya disebabkan oleh interaksi yang salah antara pengguna dengan sensor biometrik dan dapat dengan mudah diperbaiki dengan mengizinkan pengguna untuk menampilkan kembali ciri biometriknya. Skenario ini mirip dengan kasus ketika pengguna dalam sistem autentikasi berbasis kata sandi membuat kesalahan saat memasukkan kata sandi dan diizinkan untuk memasukkan kembali kata sandi tersebut.

Tingkat Kecocokan Palsu sebesar 0,02% menunjukkan bahwa rata-rata, 1 dari 5.000 upaya autentikasi oleh penipu acak cenderung berhasil. Wajar saja untuk mempertimbangkan bagaimana FMR sistem biometrik dibandingkan dengan keamanan yang disediakan oleh sistem berbasis kata sandi. Pertimbangkan sistem autentikasi berbasis pengetahuan sederhana yang menggunakan PIN numerik empat digit. Karena PIN 4 digit dapat memuat 10.000 nilai yang berbeda, rata-rata diperlukan 5.000 upaya penipu untuk menebak PIN dengan benar.

Apakah ini berarti bahwa keamanan sistem biometrik yang beroperasi pada 0,02% FMR setara dengan keamanan yang disediakan oleh PIN 4 digit? Jawabannya tidak karena dua alasan. Pertama, perlu dicatat bahwa keamanan efektif yang disediakan oleh PIN 4 digit biasanya jauh lebih kecil dari 1 keberhasilan dalam 5.000 upaya penipu, karena sebagian besar pengguna cenderung menggunakan angka yang mudah diingat (misalnya, 1234, tahun lahir, dll.) dan PIN tersebut dapat dengan mudah ditebak oleh musuh dalam beberapa kali percobaan.

Kedua, sementara satu musuh secara teoritis dapat mencoba sejumlah tebakan untuk PIN, ia hanya memiliki sejumlah sampel biometrik yang terbatas (katakanlah sepuluh jari atau dua iris) yang dapat dicoba secara fisik. Untuk mengatasi keterbatasan ini, musuh dapat menggunakan basis data sampel biometrik atau templat offline. Namun, untuk memasukkan sampel/templat ini, ia harus menghindari komponen fisik dalam sistem biometrik (sensor, ekstraktor fitur, atau saluran komunikasi). Penghindaran ini dapat menjadi sangat sulit dengan mengamankan infrastruktur fisik sistem biometrik.

Tingkat kesalahan sistem verifikasi

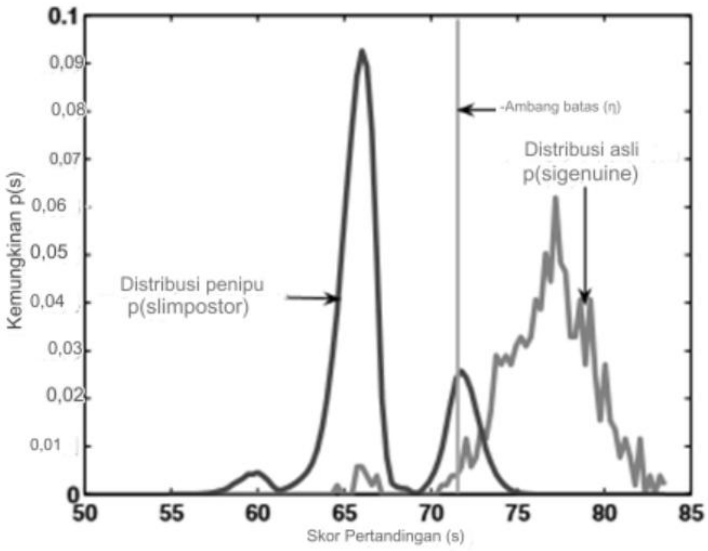
Dalam konteks verifikasi biometrik, FNMR dan FMR secara umum disebut sebagai *False Reject Rate* (FRR) dan *False Accept Rate* (FAR). Secara tegas, FMR dan FNMR tidak selalu identik dengan FAR dan FRR. Hal ini karena meskipun FNMR dan FMR diukur sebagai proporsi dari jumlah upaya pencocokan biometrik, FAR dan FRR adalah metrik tingkat aplikasi yang mengukur proporsi transaksi yang berhasil atau gagal (transaksi dapat melibatkan satu atau beberapa upaya pencocokan). Namun, dalam buku ini kami memperlakukan keduanya sebagai hal yang setara.

Skor kecocokan disebut sebagai skor asli atau autentik jika menunjukkan kesamaan antara dua sampel pasangan. Skor penipu mengukur kesamaan antara dua sampel non-pasangan. Seperti yang dibahas di bagian 1.3, sistem verifikasi membuat keputusan dengan

membandingkan skor kecocokan dengan ambang batas η. Oleh karena itu, dengan mempertimbangkan serangkaian skor kecocokan asli dan palsu, FRR dapat didefinisikan sebagai proporsi skor asli yang kurang dari ambang batas η dan FAR dapat didefinisikan sebagai fraksi skor palsu yang lebih besar atau sama dengan η.

Pertimbangkan skenario saat data biometrik (misalnya, sidik jari telunjuk kanan) yang sesuai dengan N pengguna diperoleh. Lebih lanjut, asumsikan bahwa setiap pengguna diminta untuk memberikan t sampel data biometrik mereka. Untuk menghasilkan skor kecocokan asli, sepasang sampel dari pengguna yang sama harus dibandingkan menggunakan pencocok; untuk menghasilkan skor kecocokan palsu, sepasang sampel dari dua pengguna yang berbeda harus dibandingkan. Jadi, dengan menggunakan data biometrik ini, total $Nt(t-1)/2$ skor asli dan $(N(N-1)t^2)/2$ skor palsu dapat dihasilkan oleh pencocok. Di sini, diasumsikan bahwa pencocokan tersebut simetris dalam arti bahwa perbandingan sampel A terhadap B memberikan skor yang sama dengan perbandingan B terhadap A.

Dalam notasi matematika berikutnya, kita akan menggunakan label ω_0 dan ω_1 untuk masing-masing menunjukkan kelas penipu dan asli. Misalkan $p(s|\omega_1)$ dan $p(s|\omega_0)$ masing-masing adalah fungsi kerapatan probabilitas dari skor asli dan penipu. Gambar 1.11 mengilustrasikan distribusi skor pencocokan asli dan penipu yang sesuai dengan sistem biometrik wajah. FAR dan FRR dari sistem biometrik diberikan oleh



Gambar 1.11 Distribusi skor kecocokan asli dan palsu.

Dalam ilustrasi ini, skor kecocokan asli dan palsu berasal dari pencocok yang diidentifikasi sebagai Face-G dalam Rilis Set Skor Biometrik-1 yang disediakan oleh Institut Standar dan Teknologi Nasional (NIST). Ambang batas, η, menentukan FAR dan FRR sistem. Perhatikan bahwa mengingat kedua distribusi skor kecocokan ini, FAR dan FRR tidak dapat dikurangi secara bersamaan dengan menyesuaikan ambang batas.

$$FAR(\eta) = p(s \geq \eta|\omega_0) = \int_{\eta}^{\infty} p(s|\omega_0)\, ds \tag{1.3}$$

$$FAR(\eta) = p(s \geq \eta|\omega_1) = \int_{-\infty}^{\eta} p(s|\omega_1)\, ds \tag{1.4}$$

Baik FRR maupun FAR merupakan fungsi dari ambang batas sistem η. Jika ambang batas dinaikkan, FAR akan menurun tetapi FRR akan meningkat dan sebaliknya. Oleh karena itu, untuk sistem biometrik tertentu, tidak mungkin untuk menurunkan kedua kesalahan ini secara bersamaan dengan memvariasikan ambang batas. *Genuine Accept Rate* (GAR) atau *True Accept Rate* (TAR) dapat digunakan sebagai alternatif FRR saat melaporkan kinerja sistem verifikasi biometrik. GAR didefinisikan sebagai fraksi skor asli yang melampaui ambang batas η. Oleh karena itu,

$$GAR(\eta) = p(s \geq \eta|\omega_1) = 1 - FRR(\eta) \tag{1.5}$$

Karena sistem biometrik yang sama dapat dioperasikan pada ambang batas yang berbeda (η) tergantung pada tingkat keamanan yang berubah atau persyaratan yang berbeda dari aplikasi yang berbeda, FAR dan FRR pada nilai ambang batas η yang berbeda diukur dan diringkas dalam bentuk kurva *Detection Error Tradeoff* (DET). Kurva DET memetakan FRR terhadap FAR pada berbagai ambang batas pada skala deviasi normal dan melakukan interpolasi di antara titik-titik ini (Gambar 1.12(a)). Ketika skala linear atau logaritmik digunakan untuk memetakan tingkat kesalahan ini, maka grafik yang dihasilkan dikenal sebagai kurva *Receiver Operating Characteristic* (ROC). Dalam banyak kasus, kurva ROC memetakan GAR (bukan FRR) terhadap FAR (lihat Gambar 1.12(b) dan (c)). Dengan sekumpulan skor kecocokan $\{s_i\}_{i=1}^{L}$, di mana skor kecocokan L_1 pertama sesuai dengan kelas asli, skor kecocokan L_0 berikutnya sesuai dengan kelas penipu, dan jumlah total skor adalah $L = (L_1 + L_0)$, kurva ROC dapat dihitung menggunakan teknik berikut:

1. Hasilkan satu set ambang batas $\{\eta_j\}_{j=1}^{T}$ sedemikian rupa sehingga $s_{min} \leq \eta_j \leq s_{max}, \forall_j = 1,2, \ldots, T$ di mana s_{min} dan s_{max} masing-masing adalah skor minimum dan maksimum dalam set skor kecocokan yang diberikan. Pendekatan yang umum adalah memilih ambang batas yang diberi jarak yang sama, yaitu, $\eta_j = s_{min} + (j-1)p$, di mana $p = (s_{max} - s_{min})/(T-1)$
2. Pada setiap ambang batas, $\eta_j, j = 1, 2, \ldots T.$, hitung FAR dan FRR sebagai berikut.

$$FAR(\eta_j) = \frac{1}{L_0} \sum_{i=L_{1+1}}^{L} I(s_i \geq \eta_j) \tag{1.6}$$

$$FRR(\eta_j) = \frac{1}{L_1} \sum_{i=l}^{L_1} I(s_i < \eta_j)\text{, di mana} \tag{1.7}$$

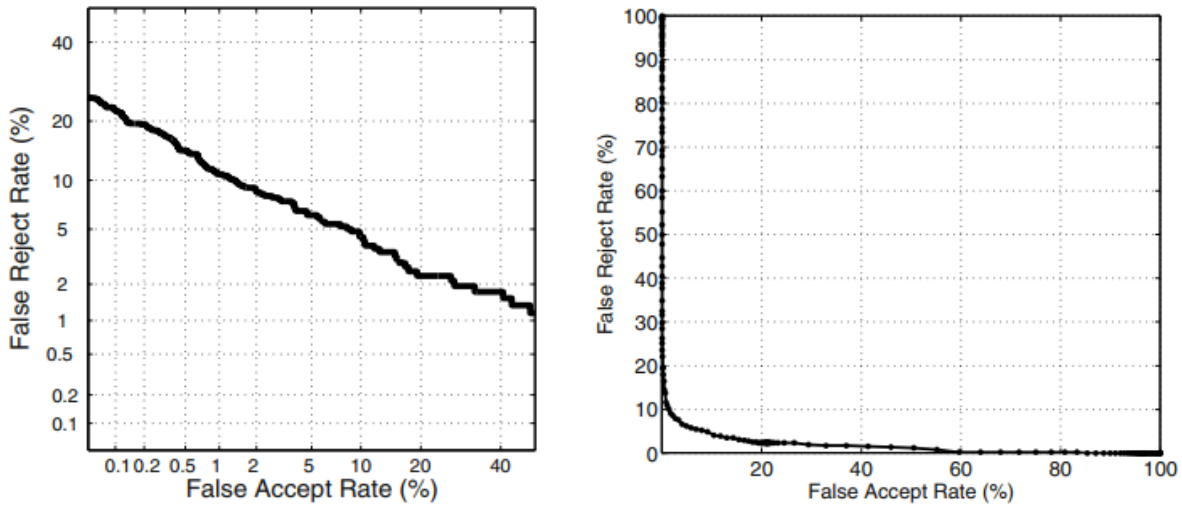
$$l(x) = \begin{cases} 1, \text{jika } x \text{ benar} \\ 0, \text{Lainnya} \end{cases} \tag{1.8}$$

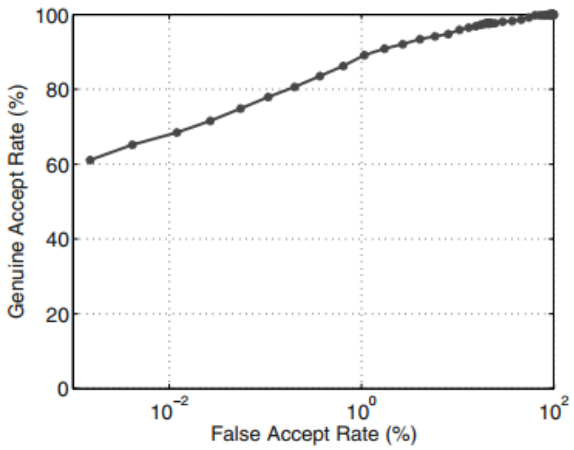
3. Kumpulan titik $\{(FAR(\eta_j), FRR(\eta_j))\}_{j=1}^{T}$, yang dihubungkan menggunakan kurva halus menghasilkan kurva ROC.

Cara terbaik untuk membandingkan kinerja dua sistem biometrik adalah dengan memeriksa kurva ROC-nya. Jika FRR dari satu sistem biometrik (misalkan A) secara konsisten lebih rendah daripada FRR dari sistem lainnya (misalkan B) untuk nilai FAR yang sesuai, seseorang dapat menyimpulkan bahwa kinerja pencocokan sistem biometrik A lebih baik daripada B. Namun, jika kedua kurva ROC berpotongan, ini menunjukkan bahwa sistem A lebih baik daripada sistem B pada beberapa titik operasi (nilai FAR), sementara sistem B lebih baik pada titik operasi lainnya. Dalam skenario ini, juga memungkinkan untuk membandingkan kinerja kedua sistem dengan memperkirakan area di bawah kurva ROC (AUC). Untuk serangkaian skor pencocokan tertentu, AUC dihitung sebagai

$$AUC = \frac{\sum_{i=1}^{L_1} \sum_{j=L1+1}^{L} I(s_i > s_j)}{L_0 L_1} \tag{1.9}$$

Nilai AUC berkisar antara 0,5 hingga 1, dengan 1 menunjukkan tidak ada kesalahan.





(c)

Gambar 1.12 Kinerja sistem verifikasi biometrik dapat diringkas menggunakan kurva DET dan ROC.

Dalam contoh ini, kurva kinerja dihitung menggunakan skor kecocokan pencocok Face-G dari Biometric Score Set Release-1 yang disediakan oleh NIST. Grafik pada (a) menunjukkan kurva DET yang memetakan FRR terhadap FAR dalam skala deviasi normal. Pada (b) kurva ROC memetakan FRR terhadap FAR dalam skala linier, sedangkan pada (c) kurva ROC memetakan GAR terhadap FAR, di mana FAR berada dalam skala logaritmik.

Penting untuk dicatat bahwa kemunculan penerimaan palsu dan penolakan palsu tidak terdistribusi secara merata di antara pengguna sistem biometrik. Ada perbedaan inheren dalam "kemampuan dikenali" dari berbagai pengguna. Empat kategori pengguna biasanya didefinisikan dalam literatur biometrik berdasarkan perbedaan inheren ini. Meskipun kategorisasi ini (yang lebih dikenal sebagai kebun binatang Doddington) awalnya dibuat dalam konteks pengenalan pembicara, kategorisasi ini juga berlaku untuk modalitas biometrik lainnya. Keempat kategori tersebut adalah:

1. Domba mewakili pengguna yang kumpulan fitur biometriknya sangat khas dan menunjukkan variasi intrakelas yang rendah. Oleh karena itu, pengguna ini diperkirakan memiliki kesalahan penerimaan palsu dan penolakan palsu yang rendah.
2. Kambing merujuk pada pengguna yang rentan terhadap penolakan palsu. Kumpulan fitur biometrik pengguna tersebut biasanya menunjukkan variasi intrakelas yang besar.
3. Domba adalah pengguna yang fitur biometriknya sangat tumpang tindih dengan fitur biometrik individu lain. Fitur biometrik pengguna ini memiliki kesamaan antarpengguna yang tinggi. Dengan demikian, pengguna yang dipilih secara acak (dari populasi target) memiliki kemungkinan lebih tinggi untuk diterima sebagai domba daripada domba jantan. Tingkat penerimaan palsu yang terkait dengan pengguna ini biasanya tinggi.
4. Serigala menunjukkan individu yang berhasil memanipulasi sifat biometrik mereka secara sengaja (terutama sifat perilaku) untuk menyamar sebagai pengguna sistem yang terdaftar secara sah. Karena serigala melakukan upaya bersama untuk mengadopsi identitas pengguna lain, upaya tersebut sering disebut sebagai serangan

musuh dan dapat meningkatkan FAR suatu sistem. Contohnya termasuk memalsukan tanda tangan pengguna lain atau meniru suara orang lain. Ini berbeda dengan serangan tanpa upaya, di mana sifat biometrik penyusup oportunistik mungkin cukup mirip dengan pengguna yang terdaftar secara sah.

Selain kesalahan false non-match dan false match, dua jenis kegagalan lainnya juga mungkin terjadi dalam sistem biometrik praktis. Jika seorang individu tidak dapat berinteraksi dengan benar dengan antarmuka pengguna biometrik atau jika sampel biometrik individu tersebut secara inheren memiliki kualitas yang sangat buruk (lihat Gambar 1.13), sensor atau ekstraktor fitur mungkin tidak dapat memproses individu-individu ini.

Sistem biometrik sidik jari, misalnya, mungkin gagal mengekstraksi fitur-fitur kecil dalam gambar yang diperoleh dari sebagian orang yang mungkin memiliki luka atau memar di jari mereka, atau yang sidik jarinya aus karena usia atau kerja manual yang berat. Oleh karena itu, pengguna tersebut tidak dapat didaftarkan dalam sistem biometrik. Tingkat Kegagalan Mendaftar (FTE) menunjukkan proporsi pengguna yang tidak dapat berhasil didaftarkan dalam sistem biometrik. Pelatihan atau pembiasaan pengguna mungkin diperlukan untuk memastikan bahwa seorang individu berinteraksi dengan sistem biometrik dengan tepat untuk memfasilitasi perolehan data biometrik berkualitas baik. Hal ini memerlukan desain antarmuka pengguna yang kuat dan efisien yang dapat membantu individu selama pendaftaran dan pengenalan.

(e) (f)

Gambar 1.13 Contoh sampel biometrik yang menyebabkan kesalahan pendaftaran.

(a) dan (b) masing-masing menunjukkan contoh jari dan tangan yang rusak, (c) dan (d) masing-masing menunjukkan contoh orang yang kehilangan jari, dan (e) dan (f) masing-masing menunjukkan mata yang rusak dan orang yang menderita penyakit mata. (Sumber: Unique Identification Authority of India)

Dalam beberapa kasus, sampel tertentu yang diberikan oleh pengguna selama autentikasi tidak dapat diperoleh atau diproses dengan andal. Jenis kesalahan ini biasanya terjadi ketika perangkat tidak dapat menemukan sinyal biometrik dengan kualitas yang cukup baik (misalnya, sidik jari yang sangat samar atau gambar wajah yang tertutup). Kesalahan ini disebut kegagalan untuk menangkap dan sebagian dari upaya autentikasi di mana sensor biometrik tidak dapat menangkap sampel yang disajikan kepadanya dikenal sebagai tingkat Kegagalan untuk Menangkap (FTC) atau Kegagalan untuk Memperoleh (FTA). Tingkat FTA juga dipengaruhi oleh keausan sensor. Dengan demikian, pemeliharaan sensor berkala sangat penting untuk fungsi sistem biometrik yang efisien.

Ada tradeoff antara tingkat FTE dan akurasi sistem yang dirasakan sebagaimana diukur oleh FAR/FRR. Kesalahan FTE biasanya terjadi ketika sistem menolak input berkualitas buruk selama pendaftaran; akibatnya, jika ambang batas kualitas tinggi, basis data sistem hanya berisi templat kualitas baik dan keakuratan sistem yang dirasakan meningkat. Karena saling ketergantungan antara tingkat kegagalan dan tingkat kesalahan, semua tingkat ini (yaitu, FTE, FTC, FAR, dan FRR) merupakan spesifikasi kinerja penting dari sistem biometrik, dan harus dilaporkan selama evaluasi sistem bersama dengan demografi populasi target (misalnya, usia, etnis, pekerjaan) yang menggunakan sistem.

Kinerja sistem biometrik juga dapat diringkas menggunakan ukuran bernilai tunggal lainnya seperti Equal Error Rate (EER) dan nilai d-prime. EER merujuk pada titik dalam kurva DET (atau ROC) di mana FAR sama dengan FRR; oleh karena itu, nilai EER yang lebih rendah menunjukkan kinerja yang lebih baik. Nilai d-prime (d') mengukur pemisahan antara rata-rata distribusi probabilitas asli dan palsu dalam satuan deviasi standar dan didefinisikan sebagai,

$$d' = \frac{\sqrt{2}|\mu_1 - \mu_0|}{\sqrt{\sigma_1 + \sigma_0}}. \qquad (1.10)$$

di mana μ_1 (μ_0) dan σ_1 (σ_0) masing-masing adalah rata-rata dan simpangan baku dari distribusi skor asli (penipu). Nilai d-prima yang lebih tinggi menunjukkan kinerja yang lebih baik. Jika distribusi asli dan penipu benar-benar mengikuti distribusi normal (Gaussian) dengan varians yang sama (situasi yang sangat tidak mungkin dalam sistem biometrik praktis), maka d' berkurang menjadi nilai simpangan baku. Ukuran kinerja bernilai tunggal lainnya dikenal sebagai Rasio-F, yang didefinisikan sebagai,

$$F - rasio = \frac{\mu_1 - \mu_0}{\sigma_1 + \sigma_0}. \tag{1.11}$$

Jika distribusi asli dan palsu adalah Gaussian, maka EER dan rasio F terkait menurut ekspresi berikut:

$$EER = \frac{1}{2} - \frac{1}{2}\text{erf}\left(\frac{F - rasio}{\sqrt{2}}\right), \tag{1.12}$$

Di mana

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,dt \tag{1.13}$$

Tingkat kesalahan sistem identifikasi

Misalkan sistem identifikasi biometrik, dengan N identitas yang terdaftar, mengeluarkan serangkaian identitas yang sesuai dengan t kecocokan teratas ($1 \le t \ll N$). Peringkat identifikasi didefinisikan sebagai peringkat identitas pengguna yang benar dalam t kecocokan teratas yang dikembalikan oleh sistem identifikasi. Misalnya, jika identitas pengguna yang benar sesuai dengan kecocokan teratas (skor tertinggi di antara semua skor kecocokan N), kami katakan bahwa pengguna telah diidentifikasi pada peringkat satu. Mirip dengan skenario verifikasi, ada dua jenis kesalahan sistem identifikasi.

Identifikasi positif palsu terjadi ketika identitas dikembalikan untuk pengguna yang tidak terdaftar dalam sistem. Ini analog dengan kasus kecocokan palsu dalam verifikasi biometrik. Proporsi transaksi identifikasi yang diharapkan oleh pengguna yang tidak terdaftar dalam sistem, di mana identitas dikembalikan, dikenal sebagai rasio identifikasi positif palsu (FPIR). FPIR bergantung pada ukuran basis data pendaftaran (N) dan ambang batas (η) yang digunakan dalam persamaan (1.2). Identifikasi negatif palsu mengacu pada skenario di mana pengguna yang bertransaksi terdaftar dalam basis data, tetapi identitasnya yang benar tidak ada di antara yang dikembalikan oleh sistem. Proporsi transaksi identifikasi yang diharapkan oleh pengguna yang terdaftar dalam sistem di mana identitas pengguna yang benar tidak dikembalikan disebut rasio identifikasi negatif palsu (FNIR).

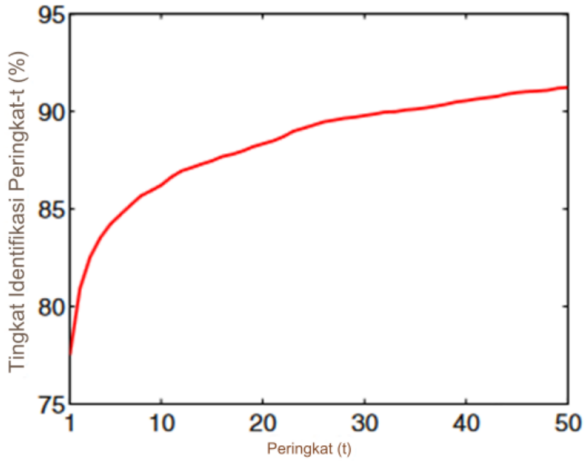
FNIR bergantung pada ukuran basis data pendaftaran (N), ambang batas (η) yang digunakan untuk skor kecocokan, dan jumlah identitas t yang dikembalikan oleh sistem identifikasi. Besaran yang terkait dengan FNIR adalah true positive identifier rate (TPIR), yang

merupakan proporsi transaksi identifikasi yang diharapkan oleh pengguna yang terdaftar dalam sistem, di mana identitas pengguna yang benar ada di antara t identitas yang dikembalikan oleh sistem. Oleh karena itu, FNIR = 1 – TPIR. Jika sistem biometrik mengeluarkan identitas dari t kecocokan teratas, TPIR yang sesuai juga dikenal sebagai rank-t identifier rate, yang kami sebut sebagai Rt. Secara khusus, nilai TPIR untuk $t = 1$ disebut akurasi peringkat satu dan nilai ini adalah salah satu metrik yang paling umum digunakan untuk membandingkan berbagai sistem identifikasi biometrik.

Tingkat identifikasi peringkat-t untuk berbagai nilai t dapat diringkas menggunakan kurva Karakteristik Pencocokan Kumulatif (CMC) (lihat Gambar 1.14), yang memplot Rt terhadap t untuk $t = 1, 2, \dots, N$, di mana N adalah jumlah pengguna yang terdaftar. Secara umum, sulit untuk menyimpulkan tingkat kesalahan identifikasi (FPIR dan FNIR) dari FMR dan FNMR dari pencocok biometrik yang mendasarinya. Ini karena identifikasi melibatkan pencarian kecocokan teratas di antara N identitas selain membandingkan skor kecocokan teratas dengan ambang batas. Namun, di bawah beberapa asumsi penyederhanaan, dimungkinkan untuk memperkirakan kinerja dalam mode identifikasi dari FMR dan FNMR dari pencocok biometrik. Misalkan sistem identifikasi mengembalikan semua identitas yang skor kecocokannya di atas ambang batas dan identitas ini ditemukan dengan membandingkan kueri secara berurutan dengan masing-masing N templat dalam basis data pendaftaran. Mari kita asumsikan juga bahwa ambang kecocokan yang sama (η) digunakan untuk skenario verifikasi dan identifikasi. Berdasarkan asumsi ini,

- ✓ FNIR = FNMR; faktanya, probabilitas bahwa input dinyatakan salah sebagai ketidakcocokan terhadap templat pengguna sama seperti dalam mode verifikasi. Dalam sebagian besar sistem identifikasi, jumlah identitas yang dikembalikan dibatasi hingga t karena kendala praktis. Ketika t kurang dari jumlah identitas yang skornya di atas ambang batas, FNIR ≥ FNMR.
- ✓ FPIR = 1 − (1 − FMR)^N ; faktanya, identifikasi positif palsu terjadi ketika input secara salah cocok dengan satu atau lebih templat dalam basis data. FPIR kemudian dihitung sebagai satu dikurangi probabilitas tidak ada kecocokan palsu yang dibuat dengan salah satu templat basis data. Dalam ekspresi di atas, $(1 - \mathrm{FMR})$ adalah probabilitas bahwa kueri tidak salah mencocokkan satu templat non-mate, dan (1 – FMR)^N adalah probabilitas tidak salah mencocokkan dengan salah satu dari N templat basis data.

Di sini, kami berasumsi bahwa semua N kecocokan bersifat independen secara statistik. Jika kami selanjutnya berasumsi bahwa FMR sangat kecil (<< $(1/N)$), FPIR dapat didekati sebagai FPIR≈ $N \times$ FMR. Dari ekspresi ini, jelas bahwa FPIR meningkat ketika nilai N meningkat dan sering kali peningkatannya bersifat linear dalam ukuran basis data (N).

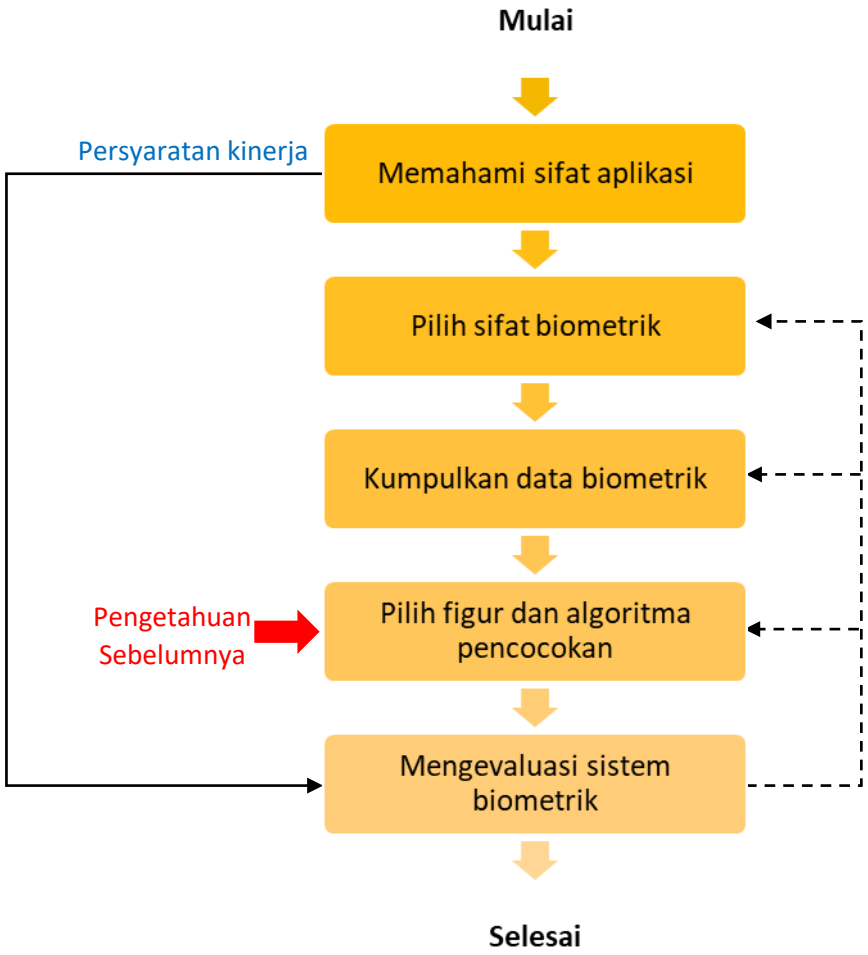


Gambar 1.14 Kurva karakteristik kecocokan kumulatif (CMC) untuk pencocok Face-G dalam Biometric Score Set Release-1 yang disediakan oleh NIST. Dalam contoh ini, rasio identifikasi peringkat-1 adalah 78%, yang berarti bahwa untuk 78% upaya identifikasi, identitas pengguna yang benar dipilih sebagai identitas yang paling cocok.

Hasil di atas menyoroti tantangan luar biasa yang terlibat dalam desain sistem identifikasi biometrik skala besar dibandingkan dengan sistem verifikasi. Sementara FMR 10^{-6} (1 kecocokan salah dalam 1 juta upaya) biasanya dapat diterima untuk pencocok biometrik yang beroperasi dalam mode verifikasi, FPIR dari sistem identifikasi dengan 10.000 pengguna terdaftar yang menggunakan pencocok dasar yang sama di bawah pengaturan ambang batas yang sama akan menjadi sekitar 1%. Andaikan saja sistem identifikasi semacam itu digunakan di bandara untuk menyaring penumpang berdasarkan daftar pantauan yang berisi 10.000 orang, 1 dari 100 penumpang yang tidak bersalah akan secara keliru dicocokkan dengan seseorang dari daftar pantauan, yang menyebabkan ketidaknyamanan dan kemungkinan rasa malu.

1.5 SIKLUS DESAIN SISTEM BIOMETRIK

Desain sistem biometrik biasanya mencakup aktivitas utama berikut, beberapa di antaranya dilakukan secara berulang. Langkah terpenting dalam mendesain sistem biometrik adalah memahami sifat aplikasi dan persyaratan kinerja. Ini diikuti dengan memilih ciri biometrik yang tepat untuk aplikasi yang sedang digunakan. Mengingat ciri biometrik tertentu, seseorang perlu mengumpulkan data biometrik dari sebagian populasi target dan mendesain atau melatih modul biometrik inti, termasuk ekstraktor fitur dan pencocok. Terakhir, sistem biometrik yang dikembangkan harus menjalani prosedur evaluasi menyeluruh untuk memastikan bahwa sistem tersebut memenuhi persyaratan aplikasi. Gambar 1.15 menyajikan ikhtisar siklus desain ini.



Gambar 1.15 Siklus desain sistem biometrik melibatkan langkah-langkah utama yang ditunjukkan di sini.

Sebagian data biometrik yang dikumpulkan selama tahap desain digunakan untuk memilih set fitur dan algoritma pencocokan yang sesuai. Bagian data yang tersisa digunakan untuk mengevaluasi apakah sistem biometrik yang dirancang memenuhi persyaratan kinerja aplikasi yang ada. Bergantung pada hasil evaluasi, beberapa langkah dalam proses di atas mungkin perlu diulang hingga diperoleh hasil yang memuaskan.

Sifat aplikasi

Desain sistem biometrik sepenuhnya bergantung pada sifat aplikasi tempat sistem biometrik akan digunakan pada akhirnya. Faktanya, karakteristik aplikasi menentukan apakah sistem biometrik diperlukan atau bahkan layak sejak awal. Sebelum memilih sistem biometrik, seseorang juga harus mempertimbangkan solusi keamanan yang ada (misalnya, kata sandi, kartu pintar, dll.) dalam domain aplikasi tempat sistem biometrik akan disematkan. Biometrik tidak harus menggantikan token dan kata sandi dalam semua aplikasi. Dalam beberapa aplikasi, biometrik dapat digunakan untuk melengkapi kartu identitas dan kata sandi, sehingga memberikan tingkat keamanan tambahan. Pengaturan seperti itu sering disebut skema autentikasi multifaktor.

Tergantung pada aplikasinya, kita mungkin perlu memilih antara fungsi verifikasi dan identifikasi. Pilihan ini tidak harus selalu saling eksklusif. Dalam beberapa aplikasi seperti

sistem ID nasional berskala besar yang memiliki cakupan penggunaan yang luas, seseorang mungkin perlu melakukan identifikasi negatif selama pendaftaran untuk mencegah kemungkinan pengguna yang sama memperoleh banyak identitas. Dalam fase pengenalan, sistem dapat berjalan dalam mode verifikasi untuk memberikan manfaat atau layanan hanya kepada pengguna yang terdaftar. Selain jenis fungsionalitas, aplikasi biometrik juga dapat diklasifikasikan berdasarkan masalah berikut.

1. **Pengguna kooperatif versus non-kooperatif**: Kerja sama mengacu pada perilaku pengguna saat berinteraksi dengan sistem. Misalnya, dalam sistem verifikasi, kepentingan terbaik pengguna asli adalah bekerja sama dengan sistem dan diterima sebagai pengguna yang sah. Aplikasi perbankan elektronik adalah contoh di mana pengguna yang terdaftar cenderung bekerja sama dengan sistem agar dikenali secara akurat. Di sisi lain, dalam sistem pengenalan negatif, pengguna mungkin tidak bekerja sama dengan sistem (misalnya, mungkin sengaja memberikan tekanan berlebihan saat menempelkan jarinya pada sensor) untuk menghindari pengenalan. Seorang teroris yang mencoba menyembunyikan identitasnya dari aplikasi pemeriksaan bandara tidak akan bekerja sama.
2. **Penerapan secara terbuka versus terselubung**: Jika pengguna menyadari bahwa dirinya sedang menjadi sasaran pengenalan biometrik, aplikasi tersebut dikategorikan sebagai terbuka. Jika pengguna tidak menyadarinya, aplikasi tersebut disebut terselubung. Pengenalan wajah dapat dengan mudah digunakan dalam aplikasi terselubung (misalnya, pengawasan), sementara pengenalan sidik jari tidak dapat digunakan dalam mode ini (kecuali untuk identifikasi kriminal berdasarkan sidik jari laten). Sebagian besar penggunaan biometrik secara komersial bersifat terbuka.
3. **Pengguna yang terbiasa versus yang tidak terbiasa**: Jika pengguna yang terdaftar cukup sering berinteraksi dengan sistem biometrik, mereka cenderung terbiasa dalam memberikan data biometrik mereka. Misalnya, aplikasi login jaringan komputer biasanya memiliki pengguna yang sudah terbiasa (setelah periode "pembiasaan" awal) karena mereka menggunakan sistem secara teratur. Namun, aplikasi SIM biasanya memiliki pengguna yang belum terbiasa karena SIM hanya diperbarui satu kali dalam jangka waktu beberapa tahun. Ini merupakan pertimbangan penting saat merancang sistem biometrik karena keakraban pengguna dengan sistem dapat memengaruhi akurasi pengenalan karena pengguna yang terbiasa cenderung memberikan data biometrik berkualitas baik.
4. **Operasi yang dihadiri versus yang tidak dihadiri**: Klasifikasi yang dihadiri versus yang tidak dihadiri mengacu pada apakah proses akuisisi data biometrik dalam suatu aplikasi diamati, dipandu, atau diawasi oleh manusia (misalnya, petugas keamanan). Lebih jauh, suatu aplikasi mungkin memiliki operasi pendaftaran yang dihadiri tetapi operasi pengenalan yang tidak dihadiri. Misalnya, aplikasi perbankan mungkin memiliki pendaftaran yang diawasi ketika kartu ATM diterbitkan kepada pengguna, tetapi penggunaan sistem biometrik berikutnya untuk transaksi ATM tidak dihadiri.

5. **Operasi yang dikendalikan versus yang tidak dikendalikan**: Dalam lingkungan yang dikendalikan, kondisi lingkungan sekitar seperti suhu, tekanan, kelembaban, kondisi pencahayaan, dll. dapat dimoderasi selama pengoperasian sistem biometrik. Biasanya, aplikasi dalam ruangan seperti login jaringan komputer beroperasi dalam lingkungan yang terkendali, sedangkan aplikasi luar ruangan seperti entri mobil tanpa kunci atau pengawasan tempat parkir beroperasi dalam lingkungan yang tidak terkendali. Klasifikasi ini juga penting bagi perancang sistem karena sensor biometrik yang lebih kuat diperlukan untuk lingkungan yang tidak terkendali.
6. **Sistem terbuka versus tertutup**: Jika templat biometrik seseorang dapat digunakan di beberapa aplikasi, sistem biometrik dapat dianggap terbuka. Misalnya, pengguna dapat menggunakan sistem pengenalan berbasis sidik jari untuk memasuki fasilitas yang aman, login jaringan komputer, perbankan elektronik, dan ATM bank. Ketika semua aplikasi ini menggunakan templat (basis data) terpisah untuk setiap aplikasi, sistem tersebut dianggap tertutup. Sistem tertutup dapat didasarkan pada templat milik sendiri sedangkan sistem terbuka akan memerlukan format data standar dan metode kompresi data untuk bertukar dan membandingkan informasi antara sistem yang berbeda (kemungkinan besar dikembangkan oleh vendor komersial yang berbeda).

Semua faktor di atas sangat memengaruhi desain sistem biometrik. Sebagian besar aplikasi biometrik komersial, seperti akses ke fasilitas aman, memiliki atribut berikut: verifikasi, kooperatif, terbuka, terbiasa, pendaftaran yang dihadiri dan autentikasi tanpa kehadiran, dan tertutup.

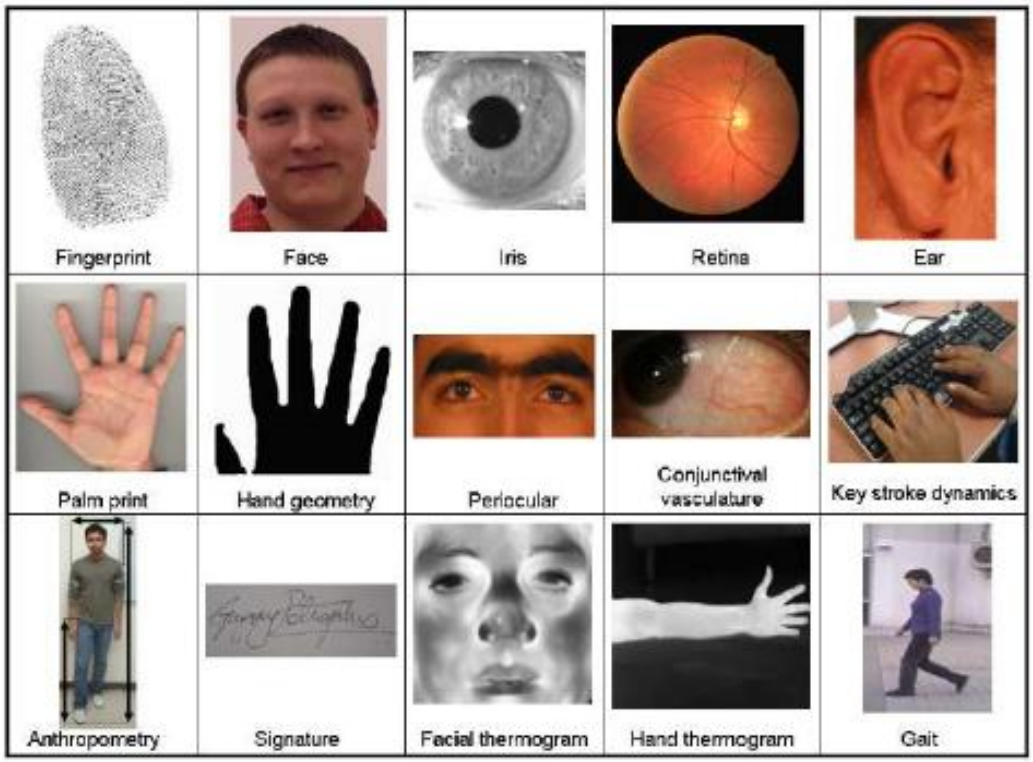
Pemilihan ciri biometrik

Sejumlah ciri biometrik digunakan dalam berbagai aplikasi. Setiap ciri biometrik memiliki kelebihan dan kekurangannya sendiri, dan oleh karena itu, pemilihan ciri biometrik untuk aplikasi tertentu bergantung pada berbagai masalah selain kinerja pengenalannya. Secara umum, tujuh faktor harus dipertimbangkan untuk menentukan kesesuaian ciri fisik atau perilaku untuk digunakan dalam aplikasi biometrik.

1. **Universalitas:** Setiap individu yang mengakses aplikasi harus memiliki ciri tersebut. Faktor ini menentukan tingkat kegagalan pendaftaran (FTE) sistem biometrik.
2. **Keunikan:** Ciri yang diberikan harus cukup berbeda di antara individu yang membentuk populasi pengguna. Jika tidak, tingkat kecocokan palsu (FAR atau FPIR) dari sistem biometrik akan sangat tinggi.
3. **Kepermanenan**: Ciri biometrik individu harus cukup invarian selama periode waktu tertentu sehubungan dengan algoritma pencocokan. Ciri yang berubah secara signifikan dari waktu ke waktu bukanlah biometrik yang berguna karena akan menyebabkan tingkat ketidakcocokan palsu yang tinggi (FRR atau FNIR).
4. **Keterukuran**: Ciri biometrik harus dapat diperoleh dan didigitalkan menggunakan perangkat yang sesuai yang tidak menyebabkan ketidaknyamanan yang tidak semestinya bagi individu. Lebih jauh, data mentah yang diperoleh harus dapat

diproses untuk mengekstrak set fitur diskriminatif. Faktor ini secara signifikan memengaruhi frekuensi kegagalan FTE dan FTA serta akurasi pengenalan.

5. **Kinerja**: Selain akurasi pengenalan (FMR, FNMR, FTE, dan FTA), sumber daya komputasi yang dibutuhkan untuk mencapai akurasi tersebut dan throughput (jumlah transaksi yang dapat diproses per satuan waktu) dari sistem biometrik juga harus memenuhi batasan yang diberlakukan oleh aplikasi.
6. **Penerimaan**: Individu dalam populasi target yang akan menggunakan aplikasi harus bersedia untuk menyajikan ciri biometrik mereka ke sistem.
7. **Pengelakan**: Ini mengacu pada kemudahan di mana ciri individu dapat ditiru menggunakan artefak (misalnya, jari palsu), dalam kasus ciri fisik, dan peniruan, dalam kasus ciri perilaku. Ini juga mengacu pada proses pengaburan, di mana pengguna secara sengaja mengubah ciri biometriknya untuk menghindari pengenalan.



Gambar 1.16 Seperangkat ciri biometrik yang umum digunakan.

Tidak ada satu pun biometrik yang diharapkan dapat secara efektif memenuhi semua persyaratan (misalnya, akurasi, kepraktisan, biaya) yang diberlakukan oleh semua aplikasi (misalnya, forensik, kontrol akses, program tunjangan pemerintah, dll.). Dengan kata lain, tidak ada biometrik yang ideal tetapi sejumlah di antaranya dapat diterima. Relevansi biometrik tertentu terhadap suatu aplikasi ditetapkan tergantung pada sifat dan persyaratan aplikasi, dan properti karakteristik biometrik. Pengantar singkat tentang beberapa karakteristik biometrik yang umum digunakan (juga ditunjukkan pada Gambar 1.16) diberikan di bawah ini:

1. **Sidik jari**: Manusia telah menggunakan sidik jari untuk identifikasi pribadi selama beberapa dekade. Sidik jari adalah pola punggungan dan lembah pada permukaan ujung jari yang pembentukannya ditentukan selama tujuh bulan pertama perkembangan janin. Meskipun sidik jari telah digunakan dalam aplikasi forensik selama lebih dari 100 tahun, munculnya pemindai sidik jari yang murah dan ringkas telah menghasilkan sejumlah besar aplikasi komersial dalam sepuluh tahun terakhir. Dalam aplikasi yang memerlukan identifikasi skala besar yang melibatkan jutaan identitas, beberapa sidik jari seseorang (misalnya, sepuluh sidik jari yang digunakan dalam Sistem Identifikasi Sidik Jari Otomatis (AFIS)) dapat digunakan untuk meningkatkan kinerja pencocokan, meskipun dengan biaya sumber daya komputasi yang lebih banyak. Akhirnya, sidik jari dari sebagian kecil populasi mungkin tidak cocok untuk identifikasi otomatis karena faktor genetik, penuaan, lingkungan, atau alasan pekerjaan (misalnya, pekerja kasar mungkin memiliki sejumlah besar luka dan memar pada sidik jarinya). Bab 2 buku ini membahas berbagai masalah yang berkaitan dengan desain dan implementasi sistem pengenalan sidik jari otomatis.
2. **Telapak tangan**: Telapak tangan manusia mengandung pola tonjolan dan lembah seperti halnya sidik jari. Area telapak tangan jauh lebih besar daripada area jari dan, sebagai hasilnya, sidik telapak tangan diharapkan lebih khas daripada sidik jari. Karena pemindai sidik telapak tangan perlu menangkap area yang luas, pemindai ini lebih besar dan lebih mahal daripada sensor sidik jari. Telapak tangan manusia juga mengandung fitur khas tambahan seperti garis-garis utama dan kerutan yang dapat ditangkap bahkan dengan pemindai resolusi rendah, yang akan lebih murah. Akhirnya, saat menggunakan pemindai sidik telapak tangan resolusi tinggi, semua fitur tangan seperti geometri, fitur tonjolan dan lembah (misalnya, hal-hal kecil dan titik-titik tunggal seperti delta), garis-garis utama, dan kerutan dapat digabungkan untuk membangun sistem biometrik yang sangat akurat. Ada minat yang meningkat dalam pencocokan sidik telapak tangan, khususnya pencocokan sidik telapak tangan laten, di antara lembaga penegak hukum. Rincian lebih lanjut tentang telapak tangan disajikan dalam Bab 2 bersama dengan sidik jari.
3. **Iris**: Iris adalah daerah melingkar mata yang dibatasi oleh pupil dan sklera (bagian putih mata) di kedua sisinya. Tekstur visual iris terbentuk selama perkembangan janin dan menjadi stabil selama dua tahun pertama kehidupan (namun, pigmentasi terus berubah selama jangka waktu yang panjang). Tekstur iris yang kompleks membawa informasi yang sangat khas yang berguna untuk pengenalan pribadi. Keakuratan dan kecepatan sistem pengenalan berbasis iris yang digunakan saat ini cukup menjanjikan dan dapat mendukung identifikasi skala besar. Meskipun sistem pengenalan berbasis iris generasi awal memerlukan partisipasi pengguna yang cukup besar dan mahal, sistem yang lebih baru telah menjadi lebih ramah pengguna dan hemat biaya. Pengenalan iris merupakan fokus utama Bab 4 buku ini.
4. **Wajah**: Pengenalan wajah merupakan metode yang tidak mengganggu, dan atribut wajah mungkin merupakan fitur biometrik yang paling umum digunakan oleh

manusia untuk mengenali satu sama lain. Aplikasi pengenalan wajah berkisar dari autentikasi "foto" yang statis dan terkendali hingga identifikasi wajah yang dinamis dan tidak terkendali di latar belakang yang berantakan. Meskipun kinerja autentikasi sistem pengenalan wajah yang tersedia secara komersial dapat diterima untuk digunakan dalam beberapa aplikasi, sistem tersebut memberlakukan sejumlah pembatasan pada cara perolehan citra wajah, yang sering kali memerlukan latar belakang yang tetap dan sederhana dengan pencahayaan yang terkendali. Sistem ini juga mengalami kesulitan dalam mencocokkan citra wajah yang diambil dari dua tampilan yang berbeda, dalam kondisi pencahayaan yang berbeda, dan pada waktu yang berbeda. Desain sistem pengenalan wajah dan tantangan terkait akan dibahas lebih rinci di Bab 3.

5. **Geometri tangan (bentuk)**: Sistem pengenalan geometri tangan didasarkan pada sejumlah pengukuran yang diambil dari tangan manusia, termasuk bentuknya, ukuran telapak tangan, dan panjang serta lebar jari-jari. Faktor lingkungan seperti cuaca kering atau anomali individu seperti kulit kering tampaknya tidak memengaruhi akurasi autentikasi sistem berbasis geometri tangan. Namun, geometri tangan tidak diketahui sangat khas dan sistem pengenalan berbasis geometri tangan tidak dapat ditingkatkan untuk sistem yang memerlukan identifikasi individu dari populasi besar. Lebih jauh, informasi geometri tangan mungkin tidak invarian selama masa pertumbuhan anak-anak. Selain itu, individu yang mengenakan perhiasan (misalnya, cincin) atau dengan keterbatasan ketangkasan (misalnya, dari radang sendi), dapat menimbulkan tantangan dalam mengekstraksi informasi geometri tangan yang benar. Ukuran fisik sistem berbasis geometri tangan besar, dan tidak dapat disematkan di perangkat tertentu seperti laptop. Ada beberapa sistem yang tersedia secara komersial yang didasarkan pada pengukuran hanya beberapa jari (biasanya, telunjuk dan tengah) dan bukan seluruh tangan. Perangkat ini lebih kecil daripada yang digunakan untuk geometri tangan, tetapi masih jauh lebih besar daripada yang digunakan untuk memperoleh ciri-ciri lain seperti sidik jari, wajah, dan suara. Biometrik bentuk tangan dibahas dalam Bab 5.
6. **Gaya berjalan**: Gaya berjalan mengacu pada cara seseorang berjalan, dan merupakan salah satu dari sedikit ciri biometrik yang dapat digunakan untuk mengenali orang dari kejauhan. Oleh karena itu, ciri ini sangat tepat dalam skenario pengawasan di mana identitas seseorang dapat ditetapkan secara rahasia. Sebagian besar algoritma pengenalan gaya berjalan mencoba mengekstrak siluet manusia untuk memperoleh atribut spasiotemporal seseorang yang sedang berjalan. Oleh karena itu, pemilihan model yang baik untuk mewakili tubuh manusia sangat penting bagi kinerja sistem pengenalan gaya berjalan yang efisien. Beberapa algoritma menggunakan aliran optik yang terkait dengan serangkaian titik bergerak yang diekstraksi secara dinamis pada tubuh manusia untuk menggambarkan gaya berjalan seseorang. Sistem berbasis gaya berjalan juga menawarkan kemungkinan untuk melacak seseorang dalam jangka waktu yang lama. Namun, gaya berjalan seseorang dipengaruhi oleh beberapa faktor,

termasuk pilihan alas kaki, jenis pakaian, kondisi kaki, dan permukaan jalan. Masalah segmentasi sangat parah untuk pengenalan berbasis gaya berjalan. Rincian lebih lanjut diberikan dalam Bab 5.

7. **Telinga**: Telah dikemukakan bahwa bentuk telinga dan struktur jaringan tulang rawan pada daun telinga bersifat khas. Pendekatan pengenalan telinga didasarkan pada pencocokan jarak titik-titik penting pada daun telinga dari lokasi penting di telinga atau berdasarkan tampilan telinga. Pengenalan telinga dapat berguna untuk mengidentifikasi seseorang berdasarkan foto profil. Lihat Bab 5 untuk detail lebih lanjut tentang sistem biometrik telinga.
8. **Suara**: Suara merupakan kombinasi karakteristik biometrik fisik dan perilaku. Ciri fisik suara seseorang didasarkan pada bentuk dan ukuran pelengkap (misalnya, saluran vokal, mulut, rongga hidung, dan bibir) yang digunakan dalam sintesis suara. Karakteristik fisik ucapan manusia ini tidak berubah untuk setiap individu, tetapi aspek perilaku ucapan berubah seiring waktu karena usia, kondisi medis (seperti flu biasa), keadaan emosional, dll. Suara juga tidak terlalu khas dan mungkin tidak sesuai untuk identifikasi skala besar. Sistem pengenalan suara yang bergantung pada teks didasarkan pada pengucapan frasa yang telah ditentukan sebelumnya. Sistem pengenalan suara yang tidak bergantung pada teks mengenali pembicara terlepas dari apa yang diucapkannya. Sistem yang dipicu teks meminta pengguna untuk mengulang frasa yang dibuat secara dinamis, yang menawarkan perlindungan lebih terhadap penipuan. Kerugian dari pengenalan berbasis suara adalah bahwa fitur ucapan sangat sensitif terhadap faktor-faktor seperti kebisingan latar belakang dan karakteristik mikrofon. Pengenalan pembicara paling tepat dalam aplikasi berbasis telepon tetapi sinyal suara biasanya diturunkan kualitasnya oleh saluran komunikasi.
9. **Penekanan tombol**: Dihipotesiskan bahwa setiap orang mengetik pada papan ketik dengan cara yang khas. Biometrik ini tidak diharapkan unik untuk setiap individu tetapi diharapkan dapat memberikan informasi diskriminatif yang cukup untuk memungkinkan verifikasi identitas. Dinamika penekanan tombol adalah biometrik perilaku; seseorang mungkin mengamati variasi intra-kelas yang besar dalam pola pengetikan seseorang karena perubahan keadaan emosional, posisi pengguna terhadap papan ketik, jenis papan ketik yang digunakan, dll. Penekanan tombol seseorang dapat dipantau secara diam-diam saat orang tersebut mengetik informasi. Hal ini memungkinkan untuk "memverifikasi secara terus-menerus" identitas seseorang selama sesi, setelah orang tersebut masuk menggunakan biometrik yang lebih kuat seperti sidik jari atau iris.
10. **Tanda tangan**: Cara seseorang menandatangani namanya diketahui sebagai karakteristik individu tersebut. Meskipun tanda tangan memerlukan kontak dengan alat tulis dan upaya dari pihak pengguna, tanda tangan telah diterima dalam transaksi pemerintah, hukum, dan komersial sebagai metode otentikasi. Dengan menjamurnya PDA, Tablet PC, dan telepon pintar, tanda tangan daring dapat muncul sebagai biometrik pilihan dalam perangkat ini. Tanda tangan adalah biometrik

perilaku yang berubah selama periode waktu tertentu dan dipengaruhi oleh kondisi fisik dan emosional penanda tangan. Tanda tangan beberapa orang sangat bervariasi: bahkan cetakan tanda tangan mereka yang berurutan pun sangat berbeda. Lebih jauh lagi, pemalsu profesional mungkin dapat mereproduksi tanda tangan yang dapat mengelabui sistem verifikasi tanda tangan.

11. **DNA**: DNA merujuk pada asam deoksiribonukleat yang mengandung informasi genetik yang diperlukan untuk perkembangan dan fungsi organisme hidup. DNA adalah kode unik satu dimensi untuk individualitas seseorang - kecuali fakta bahwa saudara kembar identik memiliki pola DNA yang sama. Namun, saat ini sebagian besar digunakan dalam konteks aplikasi forensik untuk identifikasi tersangka dan korban. Tiga masalah membatasi kegunaan DNA untuk beberapa aplikasi lain: (a) kontaminasi dan sensitivitas: mudah untuk mencuri sepotong DNA dari subjek yang tidak menaruh curiga yang selanjutnya dapat disalahgunakan untuk tujuan tersembunyi; (b) masalah pengenalan waktu nyata otomatis: teknologi canggih untuk pencocokan DNA memerlukan metode kimia yang rumit (proses basah) yang melibatkan keterampilan ahli dan belum diarahkan untuk pengenalan non-invasif daring; (c) masalah privasi: informasi tentang kerentanan seseorang terhadap penyakit tertentu dapat diperoleh dari pola DNA dan ada kekhawatiran bahwa penyalahgunaan informasi kode genetik yang tidak disengaja dapat mengakibatkan diskriminasi sosial, misalnya, dalam praktik perekrutan.
12. **Termogram inframerah wajah, tangan, dan pembuluh darah tangan**: Pola panas yang dipancarkan oleh tubuh manusia merupakan karakteristik individu dan dapat ditangkap oleh kamera inframerah dengan cara yang tidak mencolok seperti foto biasa (spektrum tampak). Teknologi ini juga dapat digunakan untuk pengenalan rahasia. Sistem berbasis termogram tidak memerlukan kontak dan tidak invasif, tetapi akuisisi gambar menjadi tantangan di lingkungan yang tidak terkendali, di mana permukaan yang memancarkan panas (misalnya, pemanas ruangan dan pipa knalpot kendaraan) ada di sekitar tubuh manusia. Teknologi terkait yang menggunakan pencitraan inframerah dekat (NIR) digunakan untuk memindai bagian belakang kepalan tangan untuk menentukan struktur pembuluh darah tangan. Sensor inframerah saat ini mahal, yang merupakan faktor yang menghambat penggunaan termogram secara luas. 13. Bau: Diketahui bahwa setiap objek mengeluarkan bau yang merupakan karakteristik komposisi kimianya dan ini berpotensi digunakan untuk membedakan berbagai objek. Bau udara yang mengelilingi suatu objek dihembuskan ke serangkaian sensor kimia, yang masing-masing peka terhadap kelompok senyawa (aromatik) tertentu. Komponen bau yang dikeluarkan oleh tubuh manusia (atau hewan apa pun) khas untuk individu tertentu. Tidak jelas apakah invariansi dalam bau badan dapat dideteksi meskipun ada bau deodoran, dan komposisi kimia lingkungan sekitar yang bervariasi.
13. **Pemindaian retina**: Vaskulatur retina kaya akan struktur dan seharusnya khas untuk setiap individu dan setiap mata. Diklaim sebagai biometrik paling aman karena tidak

mudah untuk mengubah atau mereplikasi pembuluh darah retina. Akuisisi gambar mengharuskan seseorang untuk mengintip ke lensa mata dan memfokuskan pada titik tertentu di bidang visual sehingga bagian pembuluh darah retina yang telah ditentukan sebelumnya dapat dicitrakan. Akuisisi gambar melibatkan kerja sama subjek, memerlukan kontak dengan lensa mata, dan memerlukan upaya sadar dari pihak pengguna. Semua faktor ini berdampak buruk pada penerimaan publik terhadap biometrik retina. Pembuluh darah retina dapat mengungkapkan beberapa kondisi medis, misalnya, hipertensi, yang merupakan faktor lain yang menghalangi penerimaan publik terhadap biometrik berbasis pemindaian retina.

Tabel 1.1 merangkum tingkat kesalahan sistem biometrik sidik jari, wajah, iris, dan suara yang diperoleh melalui berbagai uji evaluasi teknologi. Faktanya, keempat modalitas biometrik ini adalah satu-satunya yang telah menjalani pengujian dan evaluasi ekstensif sejauh ini. Meskipun tingkat kesalahan yang disajikan dalam Tabel 1.1 bergantung pada sejumlah kondisi pengujian seperti sensor yang digunakan, protokol akuisisi, jumlah dan profil demografi subjek yang terlibat, dan selang waktu antara akuisisi biometrik berturut-turut, semuanya memberikan perkiraan yang baik tentang keakuratan sistem biometrik terkini karena hasil ini diperoleh dengan pengujian pihak ketiga yang independen terhadap algoritme yang bersaing pada basis data umum. Hasil evaluasi ini dengan jelas menunjukkan bahwa sistem biometrik memiliki tingkat kesalahan yang tidak nol dan ada ruang untuk meningkatkan keakuratan sistem biometrik.

Tabel 1.1 Tingkat penolakan salah dan penerimaan salah yang terkait dengan sistem verifikasi sidik jari, wajah, suara, dan iris terkini. Perhatikan bahwa estimasi akurasi sistem biometrik bergantung pada sejumlah kondisi pengujian.

Ciri Biometrik	Tes	Kondisi Uji	Tingkat Penolakan Palsu	Tingkat penerimaan Palsu
Sidik jari	FVC Tahun 2006	Populasi heterogen termasuk pekerja kasar dan orang lanjut usia	4,2 %	O,1 %
	FpVTE Tahun 2003	Data operasional pemerintah AS	0,6 %	0,1 %
Menghadapi	FRVT tahun 2006	Pencahayaan terkendali, resolusi tinggi	0,8 – 1,6 %	0,1 %
Suara	NIST tahun 2008	Teks independen, multibahasa	12%	0,1%
Iris	ES 2006	Pencahayaan terkendali, jangkauan kualitas luas	1,1 – 1,4 %	0,1 %

Salah satu cara untuk meningkatkan akurasi sistem biometrik adalah dengan menggunakan lebih dari satu ciri biometrik dalam aplikasi pengenalan. Misalnya, ciri wajah dan iris, atau sidik jari dari kesepuluh jari seseorang dapat digunakan bersama-sama untuk

mengungkap identitas seseorang. Sistem seperti itu dikenal sebagai sistem multibiometrik. Sistem ini diharapkan lebih akurat dan andal karena tersedianya banyak bukti. Desain sistem multibiometrik akan dibahas secara rinci di Bab 6.

Pengumpulan data

Langkah berikutnya dalam siklus desain sistem biometrik adalah pengumpulan data biometrik dari sebagian populasi yang menjadi target. Data ini diperlukan untuk merancang modul ekstraksi fitur dan pencocok serta untuk mengevaluasi sistem biometrik yang dirancang. Namun, sebelum memulai pengumpulan data, pertama-tama kita perlu merancang sensor yang sesuai untuk memperoleh ciri biometrik yang dipilih. Faktor-faktor seperti ukuran, biaya, kekokohan, dan kemampuan untuk menangkap sampel biometrik berkualitas baik adalah beberapa masalah utama dalam desain sensor biometrik. Dalam kasus modalitas biometrik yang lebih matang seperti sidik jari, sensor juga harus mampu memenuhi standar industri tertentu seperti resolusi gambar minimum.

Penting untuk diingat bahwa karakteristik basis data seperti lingkungan pengumpulan data, populasi sampel, dan kebiasaan pengguna akan sangat memengaruhi kinerja sistem biometrik. Oleh karena itu, perhatian juga harus diberikan untuk memastikan bahwa basis data tersebut tidak terlalu sulit (dikumpulkan dalam kondisi yang paling buruk) atau terlalu mudah (dikumpulkan dalam kondisi yang paling menguntungkan). Jika basis data terlalu mudah (yaitu, hanya mencakup sampel biometrik berkualitas baik dengan variasi intra-pengguna yang kecil), tingkat kesalahan pengenalan yang dihasilkan akan mendekati nol dan akan sangat sulit untuk membedakan antara algoritma ekstraksi fitur dan pencocokan yang bersaing.

Di sisi lain, jika basis data terlalu sulit (yaitu, hanya mencakup sampel biometrik berkualitas buruk dengan variasi intra-pengguna yang besar), tantangan pengenalan mungkin berada di luar kemampuan teknologi yang ada. Idealnya, basis data harus mencakup sampel yang mewakili populasi dan sebaiknya menunjukkan variasi intra-kelas yang realistis (dicapai dengan mengumpulkan data selama beberapa sesi yang tersebar selama periode waktu dan dalam kondisi lingkungan yang berbeda). Lebih lanjut, karena melibatkan subjek manusia, masalah hukum dan privasi juga harus dipertimbangkan dan persetujuan organisasi seperti Institutional Review Board (IRB) wajib dilakukan di banyak negara. Hal ini membuat pengumpulan data biometrik menjadi proses yang memakan waktu, relatif mahal, dan rumit. Di sisi lain, perencanaan dan implementasi yang cermat dari proses pengumpulan data kemungkinan akan menghasilkan sistem biometrik yang berhasil dan operasional.

Pemilihan fitur dan algoritma pencocokan

Pemilihan fitur dan algoritma pencocokan yang akan digunakan merupakan salah satu langkah paling penting dalam desain sistem biometrik. Sebagian besar penelitian dan pengembangan di bidang biometrik difokuskan pada masalah ini. Desain ekstraktor dan pencocok fitur tidak hanya memerlukan basis data sampel biometrik, tetapi juga beberapa pengetahuan sebelumnya tentang sifat biometrik yang sedang dipertimbangkan. Misalnya, pengetahuan sebelumnya tentang "keunikan" titik-titik minutia memfasilitasi

pengembangan sistem pengenalan sidik jari berbasis minutia. Demikian pula, fakta bahwa pola minutia biasanya direpresentasikan sebagai serangkaian titik yang tidak berurutan, mendorong pengembangan algoritma pencocokan yang sesuai untuk mencocokkan rangkaian minutia.

Dalam beberapa modalitas biometrik, menggabungkan pengetahuan sebelumnya mungkin sulit. Pertimbangkan contoh sistem pengenalan wajah. Apa saja fitur yang membuat wajah manusia berbeda dari wajah manusia lainnya, terutama jika wajah tersebut milik individu dengan jenis kelamin dan etnis yang sama? Manusia tampaknya memiliki kemampuan untuk mempelajari perbedaan ini dengan mudah, tetapi sulit untuk memperoleh informasi ini dari manusia dan kemudian meniru proses ini dalam mesin. Karena fitur dan algoritme pencocokan sebagian besar bersifat khusus modalitas, pilihan ini akan dibahas secara rinci saat kita mempertimbangkan masing-masing modalitas dalam bab-bab berikutnya.

Faktor penting lainnya yang memengaruhi pilihan fitur dan algoritme pencocokan adalah interoperabilitas antara sistem biometrik. Sebagian besar sistem biometrik beroperasi dengan asumsi bahwa data biometrik yang akan dibandingkan diperoleh dengan menggunakan sensor yang sama dan, oleh karena itu, terbatas dalam kemampuannya untuk mencocokkan atau membandingkan data biometrik yang berasal dari sensor yang berbeda. Misalnya, sistem pengenalan pembicara mungkin merasa kesulitan untuk membandingkan sampel suara yang berasal dari dua teknologi handset (mikrofon) yang berbeda seperti electret dan carbon-button. Kinerja algoritma pengenalan wajah sangat terpengaruh ketika gambar yang digunakan untuk perbandingan diambil menggunakan jenis kamera yang berbeda. Demikian pula, sidik jari yang diperoleh menggunakan beberapa teknologi sensor tidak dapat dibandingkan secara andal karena variasi dalam teknologi sensor, resolusi gambar, area penginderaan, efek distorsi, dll.

Meskipun kemajuan telah dibuat dalam pengembangan format pertukaran data umum untuk memfasilitasi pertukaran set fitur antara vendor, sangat sedikit upaya yang telah diinvestasikan dalam pengembangan algoritma dan teknik yang sebenarnya untuk mencocokkan set fitur ini. Program US-VISIT misalnya, memperoleh informasi sidik jari (dan wajah) dari jutaan pelancong yang tiba di bandara dan pelabuhan laut AS. Sensor sidik jari optik saat ini sedang digunakan selama fase pendaftaran untuk mendapatkan gambar sidik jari. Namun, tidak ada jaminan bahwa jenis sensor yang sama akan digunakan di kemudian hari saat memverifikasi individu yang sama. Ada kemungkinan bahwa karena kemajuan dalam teknologi sensor, mungkin lebih diinginkan dan hemat biaya untuk menggunakan sensor generasi saat ini. Biaya dan waktu yang diperlukan untuk mendaftarkan ulang individu setiap kali sensor diganti akan sangat besar, dan berpotensi menyebabkan kemacetan besar dalam sistem, yang mengakibatkan ketidaknyamanan bagi pengguna. Dalam kasus seperti ini, kebutuhan akan algoritma ekstraksi dan pencocokan fitur yang beroperasi dengan lancar di berbagai sensor sangat penting dan akan berdampak signifikan pada kegunaan sistem selama jangka waktu tertentu.

Evaluasi

Evaluasi sistem biometrik lengkap adalah tugas yang kompleks dan menantang yang memerlukan pakar dari berbagai bidang, termasuk statistik, ilmu komputer, teknik, bisnis, dan psikologi, serta perancang sistem dan komunitas pengguna akhir. Untuk mendapatkan pemahaman menyeluruh tentang kinerja sistem biometrik, seseorang harus menjawab pertanyaan-pertanyaan berikut.

1. Berapa tingkat kesalahan sistem biometrik dalam aplikasi tertentu? (pencocokan atau kinerja teknis)
2. Berapa keandalan, ketersediaan, dan pemeliharaan sistem? (kinerja rekayasa)
3. Apa saja kerentanan sistem biometrik? Berapa tingkat keamanan yang disediakan sistem biometrik untuk aplikasi yang disematkan? (keamanan sistem biometrik)
4. Berapa penerimaan sistem oleh pengguna? Bagaimana sistem mengatasi masalah faktor manusia seperti masalah pembiasaan dan privasi? (kekhawatiran pengguna)
5. Berapa biaya dan hasil sistem biometrik dan manfaat nyata apa yang dapat diperoleh dari penerapannya? (laba atas investasi)

Tidak ada kerangka evaluasi biometrik yang ada yang menjawab semua pertanyaan di atas secara sistematis. Di bagian ini, kami hanya berfokus pada kinerja pencocokan sistem biometrik. Idealnya, evaluasi memerlukan pihak ketiga yang independen untuk merancang, mengelola, dan menganalisis pengujian. Kita dapat membagi evaluasi kinerja pencocokan sistem biometrik menjadi tiga tahap:

1. **Evaluasi teknologi**: Evaluasi teknologi membandingkan algoritme yang bersaing dari satu teknologi pada basis data standar. Karena basis data bersifat tetap, hasil evaluasi teknologi dapat diulang. Kompetisi Verifikasi Sidik Jari (FVC), Evaluasi Teknologi Vendor Sidik Jari (FpVTE), Uji Vendor Pengenalan Wajah (FRVT), program Teknologi Pengenalan Wajah (FERET), dan Evaluasi Pengenalan Pembicara NIST (SRE) adalah contoh evaluasi teknologi biometrik.
2. **Evaluasi skenario**: Dalam evaluasi skenario, pengujian prototipe sistem biometrik dilakukan di lingkungan yang sangat mirip dengan aplikasi dunia nyata. Karena setiap sistem akan memperoleh data biometriknya sendiri, kehati-hatian harus dilakukan untuk memastikan keseragaman dalam kondisi lingkungan dan populasi sampel di seluruh sistem prototipe yang berbeda.
3. **Evaluasi operasional**: Evaluasi operasional digunakan untuk memastikan kinerja sistem biometrik lengkap dalam lingkungan aplikasi dunia nyata tertentu pada populasi target tertentu.

Para peneliti telah mengidentifikasi beberapa praktik terbaik yang harus diikuti saat mengevaluasi kinerja teknis sistem biometrik. Ada rekomendasi yang tersedia dalam literatur biometrik tentang sejumlah masalah pengujian, termasuk ukuran pengujian, pemilihan sukarelawan, faktor-faktor yang dapat memengaruhi kinerja sistem biometrik, metodologi pengumpulan data, estimasi metrik kinerja, estimasi ketidakpastian metrik kinerja, dan pelaporan hasil kinerja. Evaluasi yang baik terhadap kinerja teknis sistem

biometrik harus mengikuti praktik terbaik ini sedekat mungkin dan menjelaskan dengan jelas setiap penyimpangan dari rekomendasi ini yang mungkin diperlukan.

1.6 APLIKASI SISTEM BIOMETRIK

Menentukan identitas seseorang dengan tingkat kepercayaan tinggi menjadi hal yang penting dalam sejumlah aplikasi di masyarakat kita yang saling terhubung. Pertanyaan seperti "Apakah dia benar-benar orang yang dia klaim?", "Apakah orang ini berwenang menggunakan fasilitas ini?" atau "Apakah dia ada dalam daftar pantauan yang ditetapkan oleh pemerintah?" secara rutin diajukan dalam berbagai skenario mulai dari penerbitan SIM hingga memasuki suatu negara. Kebutuhan akan teknik autentikasi pengguna yang andal telah meningkat seiring dengan meningkatnya kekhawatiran tentang keamanan, dan kemajuan pesat dalam jaringan, komunikasi, dan mobilitas. Dengan demikian, pengenalan biometrik semakin banyak digunakan dalam beberapa aplikasi yang berbeda. Aplikasi-aplikasi ini dapat dikategorikan ke dalam tiga kelompok utama (lihat Tabel 1.2):

1. Aplikasi komersial seperti login jaringan komputer, keamanan data elektronik, e-commerce, akses internet, penggunaan ATM atau kartu kredit, kontrol akses fisik, telepon seluler, PDA, manajemen rekam medis, pembelajaran jarak jauh, dll.
2. Aplikasi pemerintah seperti kartu identitas nasional, pengelolaan narapidana di fasilitas pemasyarakatan, SIM, jaminan sosial, pencairan tunjangan, kontrol perbatasan, kontrol paspor, dll.
3. Aplikasi forensik seperti identifikasi mayat, investigasi kriminal, anak hilang, penentuan orang tua, dll.

Tabel 1.2 Solusi pengenalan yang menggunakan biometrik dapat digunakan dalam berbagai aplikasi yang bergantung pada mekanisme pengenalan orang yang andal.

FORENSIK	PEMERINTAH	KOMERSIAL
Identifikasi mayat	Kartu tanda pengenal nasional	ATM
Investigasi kriminal	SIM; pendaftaran pemilih	Kontrol akses; login komputer
Penentuan orangtua	Pencairan tunjangan kesejahteraan	Telepon seluler
Anak hilang	Penyeberangan perbatasan	E-commerce; Internet; perbankan; kartu pintar

(a) (b)

Gambar 1.17 Sistem biometrik sedang digunakan dalam berbagai aplikasi pemerintah dan komersial.

(a) Program US-VISIT saat ini menggunakan kesepuluh sidik jari untuk memvalidasi dokumen perjalanan pengunjung ke Amerika Serikat, (b) bandara Ben Gurion di Tel Aviv menggunakan Sistem Unipass berbasis biometrik untuk keamanan, (c) program Schiphol Privium di bandara Amsterdam menggunakan pemindaian iris untuk memvalidasi identitas pelancong, (d) proyek Kartu Identitas Unik (UID) di India berencana untuk mendaftarkan 600 juta penduduk untuk memfasilitasi pengiriman berbagai skema kesejahteraan yang efisien, dan (e) informasi sidik jari digunakan di Disney World, Orlando untuk memastikan bahwa satu tiket tidak digunakan secara curang oleh banyak pengunjung, dan (f) produk baru oleh Fujitsu menangkap pola urat telapak tangan untuk verifikasi.

Contoh beberapa aplikasi yang menggunakan biometrik untuk mengautentikasi individu disajikan di bawah ini (lihat juga Gambar 1.17).

1. **Keamanan bandara**: Biometrik digunakan untuk mengautentikasi penumpang dan karyawan di berbagai bandara. Misalnya, skema Schiphol Privium di bandara Schipol Amsterdam menggunakan kartu pintar pemindai iris untuk mempercepat prosedur imigrasi. Penumpang yang terdaftar secara sukarela dalam skema ini memasukkan kartu pintar mereka di pintu gerbang dan mengintip ke kamera; kamera mengambil gambar mata penumpang dan memprosesnya untuk menemukan iris, dan menghitung serangkaian fitur; serangkaian fitur yang dihitung dibandingkan dengan data yang ada di kartu pintar untuk menyelesaikan verifikasi pengguna. Skema

serupa juga digunakan untuk memverifikasi identitas karyawan bandara Schiphol yang bekerja di area dengan keamanan tinggi. Bandara Internasional Ben Gurion di Tel Aviv telah menerapkan sistem keamanan biometrik serupa yang disebut Sistem Manajemen Bandara Unipass. Berdasarkan sistem ini, penumpang yang berangkat diharuskan memberikan sidik jari dan gambar wajah, yang disimpan dalam kartu pintar yang diberikan kepada setiap penumpang. Kartu pintar ini kemudian digunakan untuk melacak penumpang saat mereka melewati berbagai lokasi di bandara, seperti pos pemeriksaan keamanan, pemeriksaan bagasi, check-in maskapai, dan terakhir, menaiki pesawat.

2. **Aplikasi pemerintah**: Contoh bagus dari sistem biometrik skala besar adalah Teknologi Indikator Status Imigrasi dan Pengunjung Amerika Serikat (US-VISIT). Program US-VISIT merupakan salah satu langkah keamanan yang diadopsi oleh Departemen Keamanan Dalam Negeri untuk mengidentifikasi pengunjung yang memasuki Amerika Serikat. Ketika seorang pelancong dari negara bebas visa memasuki AS untuk pertama kalinya, foto wajah digital pengunjung dan sidik jari dari kesepuluh jari dikumpulkan di loket imigrasi sebelum masuk ke Amerika Serikat. Kesepuluh sidik jari tersebut dicocokkan dengan daftar pantauan dinamis yang berisi hingga beberapa juta catatan dalam waktu kurang dari 10 detik. Ini adalah contoh pengenalan negatif, yang tujuannya adalah untuk mengetahui apakah pengunjung memiliki beberapa alias. Jika tidak ada dalam daftar pantauan, pengunjung tersebut diizinkan masuk ke AS dan sidik jari orang tersebut didaftarkan ke dalam basis data pendaftaran US-VISIT untuk pencocokan di masa mendatang. Bagi pelancong yang memerlukan visa, proses di atas diselesaikan sebelum menerbitkan visa di konsulat AS. Selama kunjungan berikutnya ke Amerika Serikat, sidik jari orang tersebut dicocokkan dengan catatan sebelumnya dalam basis data pendaftaran (autentikasi) untuk memverifikasi identitas pengunjung. Lebih dari 75 juta pengunjung telah diproses melalui sistem ini sejak dimulainya pada Januari 2004 dan sekitar 1.000 telah ditolak masuk. Contoh lain dari penggunaan sistem biometrik skala besar adalah proyek Identifikasi Unik (UID) di India. Tujuan dari proyek ini adalah untuk meningkatkan secara signifikan efisiensi dan efektivitas berbagai skema penyaluran kesejahteraan yang diprakarsai oleh Pemerintah India dengan meningkatkan transparansi berbagai transaksi. Proyek ini melibatkan pengumpulan berbagai ciri biometrik, yaitu sepuluh jari, dua iris, dan wajah, serta informasi demografi (nama, jenis kelamin, tanggal lahir, dan alamat) dari penduduk India dan akan memberikan setiap penduduk nomor identifikasi unik 12 digit. Proyek ini diharapkan dapat mendaftarkan 600 juta penduduk India dalam kurun waktu lima tahun. Ini adalah contoh deduplikasi (pengenalan negatif) di mana penggabungan 10 jari dan 2 iris diharapkan dapat menentukan apakah orang yang sama mencoba memperoleh dua nomor identifikasi yang berbeda.
3. **Aplikasi komersial**: Beberapa lembaga keuangan besar di Jepang telah memasang sistem autentikasi urat nadi telapak tangan di ATM mereka untuk membantu

memvalidasi identitas nasabah yang ingin melakukan transaksi. Sensor nirkontak digunakan untuk mengambil gambar pola urat nadi di telapak tangan nasabah menggunakan sumber cahaya inframerah dekat. Contoh lain dari sistem verifikasi biometrik berthroughput tinggi adalah yang digunakan oleh Walt Disney World Resort di Orlando, Florida untuk mencegah penipuan tiket. Setiap pengunjung resor harus memberikan jari telunjuknya di pintu putar bersama dengan tiket. Sidik jari yang diberikan oleh pemegang tiket kemudian ditautkan ke tiket tertentu; jika pemegang tiket mengunjungi resor lagi (baik di kemudian hari yang sama atau di hari yang berbeda jika ia memiliki tiket masuk ganda) ia harus menunjukkan jari yang sama yang digunakan untuk memvalidasi tiket. Ini mencegah lebih dari satu orang menggunakan tiket yang sama. Sistem Disney dapat menangani sejumlah besar (sekitar 100.000 per hari) pengunjung secara efisien, dan yang lebih penting, sistem ini bekerja dalam semua kondisi cuaca karena menggunakan sensor sidik jari yang kokoh yang mampu menangkap gambar sidik jari berkualitas baik bahkan dalam kondisi pencitraan yang buruk. Rincian pribadi pengunjung tidak dikaitkan dengan data sidik jari dalam basis data, yang secara berkala dibersihkan, sehingga memberikan keamanan tanpa mengorbankan privasi.

1.7 MASALAH KEAMANAN DAN PRIVASI

Kode Amerika Serikat tentang 'Koordinasi Kebijakan Informasi Federal' mendefinisikan keamanan informasi sebagai "*melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah*". Biasanya, ada empat aspek utama yang perlu dipertimbangkan dalam keamanan informasi.

- ✓ **Integritas** - melindungi dari modifikasi atau penghancuran data yang tidak semestinya dan memastikan tidak adanya penyangkalan dan keaslian informasi.
- ✓ **Kerahasiaan data** - mencegah akses atau pengungkapan informasi sensitif yang tidak sah.
- ✓ **Ketersediaan** - menjamin akses dan penggunaan informasi yang tepat waktu dan andal.
- ✓ **Autentikasi** - hanya pengguna yang sah dan berwenang yang dapat mengakses data dan melaksanakan tugas tertentu.

Secara umum disepakati bahwa pengenalan biometrik dapat secara efektif mengatasi masalah autentikasi. Karena ciri biometrik tidak dapat dengan mudah hilang, dicuri, salah tempat, atau dibagikan, pengenalan biometrik menawarkan solusi autentikasi yang alami dan lebih andal dibandingkan dengan teknik lain seperti kata sandi atau token fisik (misalnya, kartu identitas). Inilah alasan mengapa sistem biometrik semakin banyak digunakan untuk mengendalikan akses ke sistem informasi lainnya. Misalnya, undang-undang AS mengamanatkan bahwa entitas (misalnya, penyedia layanan kesehatan, perusahaan asuransi kesehatan) yang berurusan dengan informasi kesehatan elektronik harus menerapkan prosedur autentikasi yang kuat seperti pengenalan biometrik untuk

mencegah paparan informasi kesehatan sensitif yang tidak sah. Lebih jauh lagi, dengan menerapkan skema autentikasi biometrik yang tidak dapat disangkal, akan memungkinkan untuk melacak semua akses ke informasi istimewa, sehingga meningkatkan akuntabilitas transaksi dalam sistem informasi.

Akan tetapi, penting untuk menyadari bahwa sistem biometrik hanyalah salah satu komponen dari keseluruhan solusi keamanan informasi karena sistem ini hanya menangani aspek autentikasi. Teknologi lain seperti enkripsi, tanda tangan digital, dll. diperlukan untuk memenuhi persyaratan kerahasiaan, integritas, dan ketersediaan dari keseluruhan sistem informasi. Selain itu, sistem biometrik itu sendiri dapat dianggap sebagai subsistem independen dalam keseluruhan sistem informasi. Jika sistem biometrik dikompromikan atau dielakkan, keamanan seluruh sistem informasi akan terpengaruh. Karena alasan ini, aspek keamanan yang terlibat dalam desain dan implementasi sistem biometrik perlu dianalisis dengan cermat dan independen, yang menjadi fokus Bab 7 dalam buku ini.

Pengungkapan informasi pribadi sensitif yang tidak sah dapat menyebabkan kerugian objektif (misalnya, penipuan keuangan, penolakan layanan) dan subjektif (di mana sekadar pengetahuan tentang informasi pribadi seseorang oleh pihak kedua atau ketiga dianggap sebagai cedera). Ketika pelanggaran keamanan dalam sistem informasi menyebabkan kerugian pribadi dan subjektif bagi orang yang terlibat, hal itu dapat disebut sebagai hilangnya privasi. Privasi mengacu pada hak seseorang untuk dibiarkan sendiri, yaitu, kemampuan untuk menjalani hidup sendiri tanpa gangguan, untuk tetap anonim, dan untuk mengendalikan akses ke informasi pribadi seseorang.

Meskipun kebutuhan akan privasi biasanya merupakan preferensi individu, ada beberapa kasus di mana pengungkapan informasi mungkin diperlukan demi kepentingan masyarakat yang lebih besar (misalnya, keamanan nasional). Dalam kata-kata pakar privasi Esther Dyson,

> *"Privasi bukanlah kondisi yang cocok untuk semua orang: Orang yang berbeda pada waktu yang berbeda memiliki preferensi yang berbeda tentang apa yang terjadi pada informasi pribadi mereka dan siapa yang dapat melihatnya. Daripada mencoba mendefinisikan privasi untuk semua orang, masyarakat harus memberi individu alat untuk mengendalikan penggunaan dan penyebaran data mereka. Keseimbangan antara kerahasiaan dan pengungkapan adalah preferensi individu, tetapi kebutuhan akan alat dan bahkan undang-undang untuk menerapkan preferensi itu bersifat umum."*
>
> **- - Scientific American, September 2008.**

Meskipun pengenalan biometrik dapat berfungsi sebagai alat untuk menjaga privasi individu dengan membatasi akses ke informasi pribadi mereka (misalnya, catatan medis), penggunaan biometrik itu sendiri dapat menciptakan teka-teki privasi. Ini karena pengenal biometrik menyediakan hubungan yang tak terbantahkan dengan identitas seseorang. Akibatnya, pengguna sistem biometrik memiliki sejumlah kekhawatiran yang sah.

Apakah bukti akses berbasis biometrik yang tidak dapat disangkal akan melanggar hak individu untuk tetap anonim? Misalnya, orang yang secara hukum memiliki banyak alias

(misalnya, untuk alasan keamanan) dapat diidentifikasi menggunakan pengenalan biometrik. Lebih jauh, sering kali memungkinkan untuk mengenali pengguna secara diam-diam dengan menangkap ciri-ciri biometriknya tanpa keterlibatan aktifnya (misalnya, wajah dapat ditangkap menggunakan kamera pengintai tersembunyi). Akibatnya, orang yang ingin tetap anonim dalam situasi tertentu dapat ditolak privasinya karena pengenalan biometrik.

Apakah data biometrik akan disalahgunakan untuk tujuan yang tidak diinginkan (perambatan fungsi), misalnya, memungkinkan keterkaitan catatan identitas lintas sistem tanpa sepengetahuan pengguna? Misalnya, templat sidik jari yang diperoleh dari basis data bank dapat digunakan untuk mencari catatan kesehatan orang tersebut dalam basis data medis. Bagaimana memastikan bahwa sistem informasi memang secara eksklusif menggunakan pengenalan biometrik untuk tujuan yang dimaksudkan (misalnya, dapatkah dibuktikan secara nyata bahwa administrator sistem tepercaya tidak dapat menyalahgunakan sistem)?

Apakah persyaratan biometrik akan proporsional dengan kebutuhan keamanan, misalnya, apakah sidik jari diperlukan untuk membeli hamburger di restoran cepat saji atau mengakses situs web komersial?

Siapa yang memiliki data biometrik, individu atau penyedia layanan?

Masalah privasi di atas pelik dan tidak memiliki jawaban konkret. Meskipun seseorang dapat menetapkan beberapa langkah untuk melindungi privasi pengguna, tidak ada solusi praktis yang memuaskan di masa mendatang untuk mengatasi seluruh spektrum masalah privasi atau bagaimana tepatnya masalah privasi ini perlu dipertukarkan dengan masalah keamanan. Prinsip praktik informasi yang adil seperti transparansi, persetujuan yang diinformasikan, pembatasan penggunaan, akuntabilitas, dan audit dapat diikuti untuk membatasi masalah privasi yang timbul dari pengenalan biometrik. Karena masalah ini berada di luar cakupan teknologi, undang-undang yang sesuai harus diberlakukan untuk menegakkan prinsip-prinsip ini. Pengaturan mandiri oleh industri biometrik dan penegakan aturan secara otonom oleh organisasi pengatur independen (misalnya, Otoritas Biometrik Pusat) juga dapat mengatasi ketakutan privasi masyarakat umum.

RINGKASAN

Pengenalan orang yang andal merupakan bagian penting dari berfungsinya masyarakat kita dengan baik. Sekarang sudah diterima secara luas bahwa teknik pengenalan konvensional yang didasarkan pada kredensial seperti SIM, paspor, kata sandi, atau PIN tidak cukup andal untuk mengenali seseorang karena mudah dicuri dan dipalsukan. Pengenalan biometrik, atau biometrik saja, mengacu pada pengenalan otomatis seseorang berdasarkan ciri fisik dan perilaku khasnya (misalnya, wajah, sidik jari, iris, suara). Biometrik menawarkan sejumlah keunggulan dibandingkan autentikasi berbasis token atau pengetahuan: (a) mencegah penipuan dan meningkatkan keamanan, (b) mendeteksi banyak pendaftaran, (c) tidak dapat dengan mudah dipindahkan, dilupakan, hilang, atau disalin, (d) menghilangkan klaim penolakan, dan (e) meningkatkan kenyamanan pengguna. Hasilnya, pengenalan biometrik sekarang diakui sebagai alat yang ampuh dan penting untuk manajemen identitas.

Mengingat penerapan kartu identitas nasional berbasis biometrik dan paspor elektronik baru-baru ini oleh beberapa pemerintah, sudah pasti bahwa pengenalan biometrik akan sangat memengaruhi cara kita dikenali dalam kehidupan sehari-hari. Meskipun pengenalan biometrik telah berhasil diterapkan dalam beberapa aplikasi khusus, hal itu masih jauh dari masalah yang terpecahkan. Seperti yang diamati dari Tabel 1.1, jelas ada banyak ruang untuk perbaikan dalam kinerja pencocokan teknologi biometrik. Para peneliti tidak hanya menangani masalah yang terkait dengan pengurangan tingkat kesalahan, tetapi mereka juga mencari cara untuk meningkatkan kegunaan sistem biometrik. Misalnya, penerapan biometrik dalam banyak aplikasi sipil dan pemerintah juga telah menimbulkan pertanyaan terkait privasi yang diberikan kepada individu yang terdaftar dan keamanan sistem biometrik itu sendiri. Ada juga kebutuhan yang pasti untuk standarisasi sistem biometrik untuk (a) memfasilitasi interoperabilitas antara vendor, dan (b) untuk memastikan bahwa subsistem biometrik dapat dengan mudah diintegrasikan ke dalam berbagai aplikasi.

BAB 2
PENGENALAN SIDIK JARI

"Mungkin yang paling indah dan khas dari semua tanda permukaan adalah alur kecil dengan tonjolan di antaranya dan pori-porinya yang tersusun dalam urutan yang sangat rumit namun teratur pada permukaan bawah tangan dan kaki."

Francis Galton, Nature, 28 Juni 1888.

Pola tonjolan dan lembah yang saling bertautan pada ujung jari disebut sebagai sidik jari. Penggunaan pola-pola ini secara sistematis untuk identifikasi pribadi dipromosikan pada akhir abad ke-19 hingga awal abad ke-20, meskipun penemuan sidik jari manusia pada sejumlah besar artefak arkeologi menunjukkan bahwa orang-orang kuno menyadari potensi individualitas sidik jari. Meskipun sidik jari awalnya diperoleh dengan cara menggulung ujung jari yang bertinta pada permukaan kertas, kemajuan teknologi sensor telah menghasilkan desain sensor optik dan solid-state yang ringkas dan murah yang dapat dengan cepat mengambil gambar ujung jari dan menghasilkan rendisi digital sidik jari untuk analisis otomatis. Bab ini membahas teknologi yang digunakan untuk pencitraan sidik jari, jenis fitur yang diekstraksi dari gambar digital sidik jari, teknik untuk mengklasifikasikan gambar sidik jari, dan metode untuk ekstraksi fitur otomatis dan pencocokan gambar sidik jari.

2.1 PENDAHULUAN

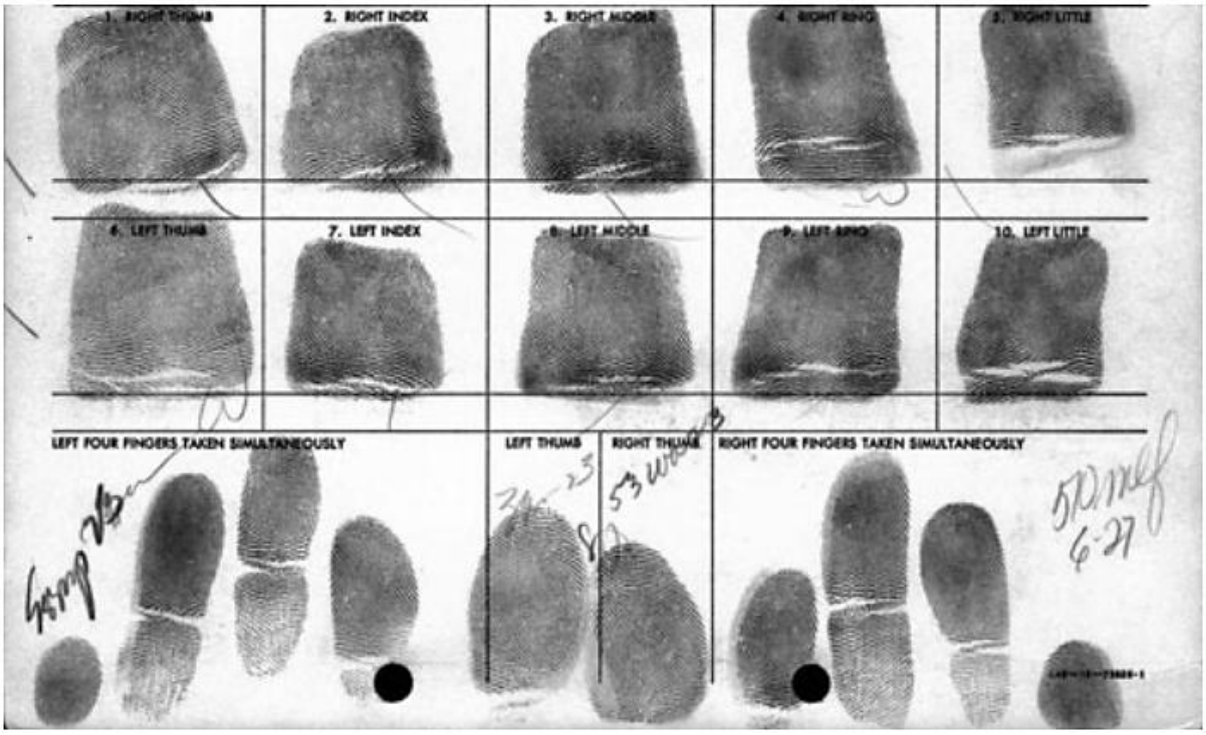
Tidak seperti kulit di sebagian besar bagian tubuh kita, yang halus dan mengandung rambut dan kelenjar minyak, kulit di telapak tangan dan telapak kaki menunjukkan pola seperti aliran berupa tonjolan dan lembah (kadang-kadang disebut alur), dan tidak mengandung rambut atau kelenjar minyak. Tonjolan papiler pada jari ini, yang disebut tonjolan gesekan, membantu tangan untuk menggenggam benda dengan meningkatkan gesekan dan meningkatkan penginderaan taktil terhadap tekstur permukaan. Kulit tonjolan gesekan terdiri dari dua lapisan utama: dermis (lapisan dalam) dan epidermis (lapisan luar). Tonjolan muncul pada epidermis untuk meningkatkan gesekan antara volar (telapak tangan atau telapak kaki) dan permukaan kontak (lihat Gambar 2.1). Rata-rata, seorang pria muda memiliki 20,7 tonjolan per sentimeter sementara seorang wanita memiliki 23,4 tonjolan per sentimeter.

Nilai penting lain dari tonjolan gesekan adalah penggunaannya dalam pengenalan biometrik. Pola tonjolan gesekan pada setiap jari (Gambar 2.1(b)) diklaim unik dan tidak dapat diubah, sehingga memungkinkan penggunaannya sebagai tanda identitas. Bahkan, saudara kembar identik pun dapat dibedakan berdasarkan sidik jari mereka. Cedera superfisial seperti luka dan memar pada permukaan jari mengubah pola di daerah yang rusak hanya untuk sementara. Memang, struktur tonjolan telah diamati muncul kembali setelah cedera sembuh. Namun, jika cedera meluas ke lapisan basal epidermis, hal itu dapat menghilangkan kemampuan lapisan basal untuk meregenerasi sel-sel di daerah yang rusak. Sementara sel-sel basal di sekitarnya akan mencoba untuk memperbaiki cedera seperti itu,

proses ini akan menghasilkan bekas luka permanen pada permukaan kulit tonjolan gesekan. Meskipun kemungkinan menggunakan sidik jari sebagai pengenal unik telah diakui ribuan tahun yang lalu, penggunaan sistematisnya dalam aplikasi yang memerlukan pengenalan orang tidak terjadi sampai awal abad ke-20. Badan penegak hukum sekarang secara rutin merekam sidik jari penjahat pada kartu sepuluh sidik jari (Gambar 2.2), yang menangkap cetakan yang digulung dan polos dari semua sepuluh sidik jari.

(a) (b)

Gambar 2.1 Ada dua jenis kulit pada tubuh manusia: (a) kulit halus dan (b) kulit beralur gesekan. Kulit beralur gesekan terlihat memiliki pola beralur yang diselingi lembah.



Gambar 2.2 Kartu sepuluh sidik jari.

Dua baris teratas menunjukkan sidik jari yang diperoleh dengan menggulung setiap jari dari satu sisi ke sisi lain (disebut sidik jari tergulung). Baris paling bawah menunjukkan sidik jari polos atau sidik jari tampar: sidik jari tampar empat jari (kelingking sampai telunjuk) tangan kiri yang diperoleh secara serentak ditunjukkan di

bagian kiri baris paling bawah, dua sidik jari ibu jari ditunjukkan di tengah, dan sidik jari tampar empat jari (telunjuk sampai kelingking) tangan kanan yang diperoleh secara serentak ditunjukkan di sebelah kanan.

Dua tujuan utama dari sidik jari yang direkam adalah (a) untuk mengidentifikasi pelanggar berulang yang sering menggunakan alias untuk menyembunyikan identitas asli mereka dan (b) untuk melakukan pemeriksaan latar belakang untuk pekerjaan atau perizinan. Aplikasi penting lain dari sidik jari dalam penegakan hukum adalah untuk menetapkan identitas tersangka berdasarkan sidik jari parsial yang tertinggal di tempat kejadian perkara. Ini disebut sidik jari laten, atau hanya laten (lihat Gambar 2.3(c)). Dibandingkan dengan sidik jari yang digulung dan polos pada Gambar 2.3(a) dan 2.3(b), laten biasanya memiliki kualitas gambar yang buruk. Ketika ukuran basis data sidik jari mulai berkembang menjadi jutaan, Sistem Identifikasi Sidik Jari Otomatis (AFIS) dikembangkan pada tahun 1970-an untuk meningkatkan efisiensi dan akurasi pencocokan sidik jari. Saat ini, hampir setiap lembaga penegak hukum di seluruh dunia mengandalkan AFIS untuk mencocokkan sidik jari. Gambar 2.4 menunjukkan AFIS yang dipasang di fasilitas Kepolisian Negara Bagian Michigan. Meningkatnya kekhawatiran tentang keamanan dalam negeri dan penipuan konsumen telah mendorong penggunaan sistem biometrik berbasis sidik jari dalam banyak aplikasi non-forensik.

(a) (b) (c)

Gambar 2.3 Tiga cetakan sidik jari yang berbeda dari jari yang sama.

(a) Sidik jari tergulung, (b) sidik jari biasa, dan (c) sidik jari laten.

Faktanya, sistem biometrik berbasis sidik jari sangat populer dan sukses sehingga menjadi sinonim dengan gagasan pengenalan biometrik di benak masyarakat umum.

Gambar 2.4 Pemasangan AFIS di fasilitas Kepolisian Negara Bagian Michigan. Sistem ini pertama kali dipasang pada tahun 1989; basis datanya memiliki 3,2 juta kartu sepuluh sidik jari dan melakukan 700.000 penelusuran setiap tahun.

2.2 POLA FRICTION RIDGE

Pengenalan sidik jari, baik yang dilakukan secara manual oleh pakar manusia atau secara otomatis oleh mesin, sebagian besar berbasis fitur (bukan berbasis gambar) dan fitur yang digunakan memiliki interpretasi fisik. Istilah berbasis fitur dan berbasis gambar banyak digunakan dalam literatur visi komputer untuk menunjukkan metode yang digunakan untuk merepresentasikan dan mencocokkan gambar seperti sidik jari. Metode berbasis fitur, seperti namanya, mengekstrak fitur eksplisit dari gambar yang dipertimbangkan dan mengodekan fitur ini ke dalam satu set fitur, yang selanjutnya digunakan untuk pencocokan. Sebaliknya, metode berbasis gambar, secara langsung menggunakan gambar untuk pencocokan tanpa mengekstrak fitur apa pun secara eksplisit darinya.

Pertama-tama kami memperkenalkan berbagai jenis fitur yang dapat diekstraksi dari sidik jari, diikuti dengan deskripsi histologi kulit friction ridge dan pembentukannya. Pengetahuan tentang kedua topik ini penting untuk memahami keunikan dan keawetan pola tonjolan gesekan, yang merupakan dua premis mendasar dalam pengenalan sidik jari.

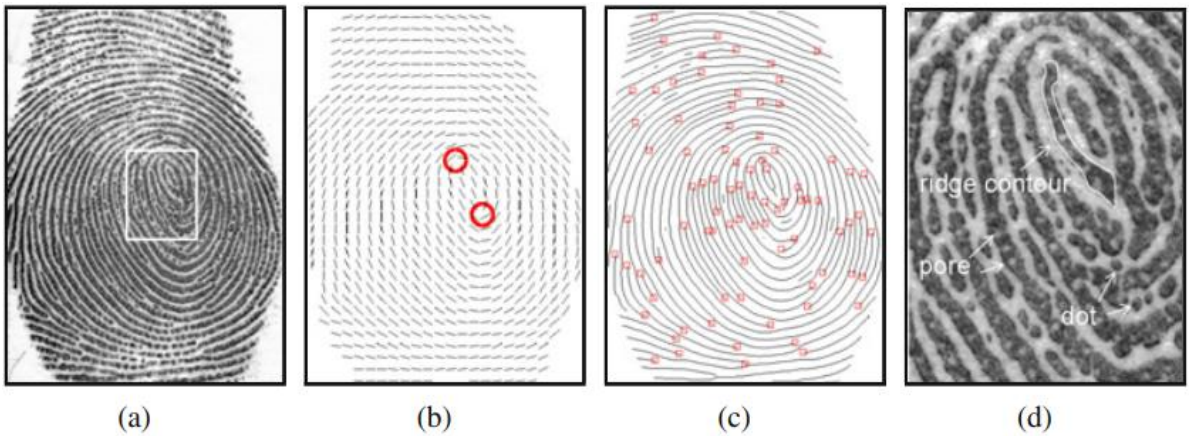
Fitur

Detail dalam sidik jari dapat dikarakterisasi pada tiga tingkat berbeda mulai dari kasar hingga halus. Dalam kondisi ideal, fitur tingkat kasar dapat diturunkan dari tingkat representasi sidik jari yang lebih halus.

Fitur level 1

Pada level pertama (paling kasar), sidik jari direpresentasikan sebagai peta orientasi punggungan (lihat Gambar 2.5(b)), yang merekam orientasi punggungan lokal di setiap lokasi sidik jari, dan peta frekuensi punggungan, yang merekam frekuensi punggungan lokal di setiap lokasi dalam sidik jari. Sidik jari sering disebut sebagai pola tekstur berorientasi karena bentuk dan struktur globalnya dapat didefinisikan oleh orientasi dan frekuensi punggungannya. Pada detail Level 1, hanya aliran punggungan dan frekuensi punggungan

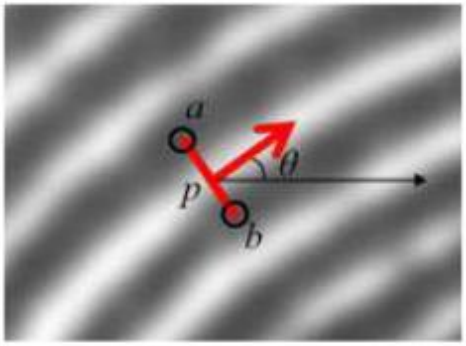
yang diamati; lokasi pasti dan detail dimensi punggungan diabaikan. Dengan demikian, sensor gambar beresolusi rendah yang mampu memindai 250 piksel per inci (ppi) dapat digunakan untuk mengamati detail Level 1 sidik jari.



Gambar 2.5 Fitur pada tiga level berbeda dalam sidik jari.

(a) Citra skala abu-abu (NIST SD30, A067 11), (b) Fitur level 1 (bidang orientasi atau aliran punggungan dan titik singular), (c) Fitur level 2 (kerangka punggungan), dan (d) Fitur level 3 (kontur punggungan, pori, dan titik).

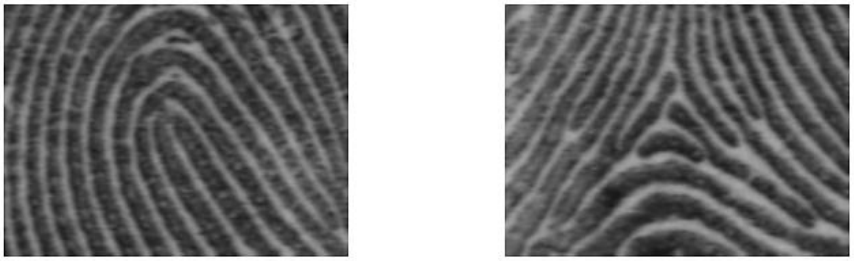
Orientasi punggungan lokal pada piksel (x, y) menunjukkan arah tangensial garis punggungan yang melewati (x, y). Orientasi punggungan didefinisikan dalam rentang [0, π). Dengan demikian, peta orientasi punggungan dapat dilihat sebagai medan vektor satuan panjang yang arahnya didefinisikan antara 0 dan π. Orientasi punggungan pada piksel p diilustrasikan dalam Gambar 2.6. Frekuensi punggungan lokal pada (x, y) adalah jumlah rata-rata punggungan per satuan panjang sepanjang segmen garis yang berpusat di (x, y) dan normal terhadap orientasi punggungan lokal. Frekuensi punggungan adalah kebalikan dari periode punggungan, yang diilustrasikan pada Gambar 2.6. Secara umum, informasi orientasi punggungan dipandang lebih penting daripada informasi frekuensi punggungan untuk tujuan pencocokan dan klasifikasi sidik jari.



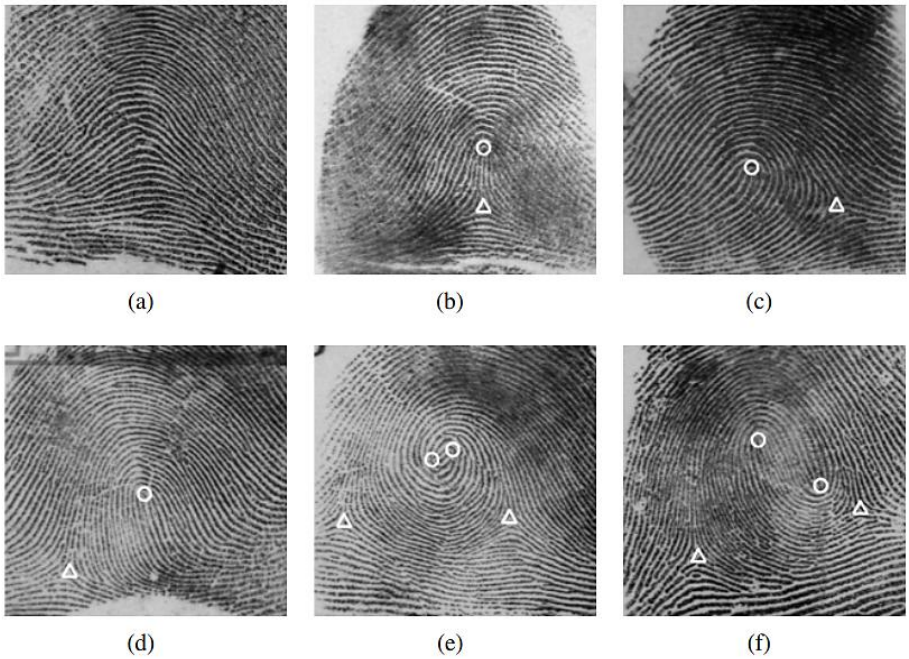
Gambar 2.6 Detail Level 1 berkaitan dengan fitur kasar sidik jari.

Detail ini menangkap orientasi punggungan dan informasi frekuensi dalam sidik jari. Gambar ini menunjukkan sebagian sidik jari dengan punggungan yang ditunjukkan sebagai garis gelap dengan orientasi punggungan θ dan periode punggungan ab (kebalikan dari frekuensi punggungan) ditandai pada piksel p.

Peta orientasi punggungan biasanya berisi beberapa lokasi menonjol tempat orientasi punggungan berubah secara tiba-tiba - lokasi tersebut disebut sebagai titik singular. Ada dua jenis dasar titik singular - loop dan delta - dan keduanya secara visual berbeda. Singularitas tipe loop, juga disebut inti, merujuk ke area lokal tempat sekumpulan punggungan masuk dari satu arah dan keluar ke arah yang sama (Gambar 2.7(a)). Loop dalam sidik jari dapat digunakan sebagai titik acuan untuk menyelaraskan sidik jari. inti Secara umum, titik inti sesuai dengan titik singular tipe loop paling utara dalam sidik jari; jika sidik jari tidak mengandung titik singular (misalnya, sidik jari tipe lengkung), inti biasanya merujuk ke titik kelengkungan punggungan maksimum. Namun, istilah inti itu sendiri sering digunakan untuk menunjukkan singularitas tipe loop dalam praktik. Singularitas tipe delta menunjukkan area lokal tempat tiga sistem punggungan tampak bertemu (Gambar 2.7(b)).



Gambar 2.7 Titik singular. (a) Loop dan (b) delta.



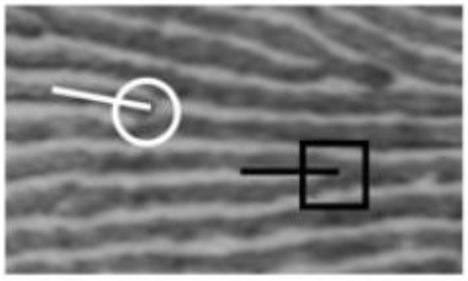
Gambar 2.8 Jenis pola sidik jari utama.

(a) Lengkungan polos, (b) lengkung tenda, (c) lengkung kiri, (d) lengkung kanan, (e) lingkaran, dan (f) lengkung kembar. Lengkung dilambangkan dengan lingkaran dan delta dilambangkan dengan segitiga. Sidik jari tipe lengkung dan lingkaran paling umum ditemukan; sekitar 65% sidik jari termasuk tipe lengkung, dan 24% adalah tipe lingkaran [52]. Lengkung kembar, lengkung, dan lengkung tenda masing-masing mencakup sekitar 4%, 4%, dan 3% dari sidik jari.

Kumpulan titik singular dalam sidik jari dapat dilihat sebagai representasi abstrak dari peta orientasi sehingga peta orientasi dapat diprediksi secara kasar berdasarkan jumlah dan lokasi titik singular. Representasi peta orientasi yang lebih abstrak lagi adalah tipe pola (sering disebut sebagai kelas sidik jari), yang dapat disimpulkan berdasarkan jumlah loop dan delta, dan hubungan spasial di antara keduanya. Contoh enam tipe pola sidik jari utama ditunjukkan pada Gambar 2.8, dan hampir semua sidik jari termasuk dalam salah satu kelas tersebut. Singularitas pada sebagian besar sidik jari diamati memenuhi batasan berikut: (a) jumlah loop dan delta dalam cetakan penuh adalah sama; dengan kata lain, loop dan delta muncul berpasangan; dan (b) jumlah total titik singular adalah 0, 2, atau 4. Prosedur untuk menentukan jenis pola sidik jari berdasarkan titik singular akan dibahas nanti dalam bab ini.

Fitur level 2

Pada level kedua (tengah), sidik jari direpresentasikan sebagai gambar kerangka punggungan yang setiap punggungannya hanya selebar satu piksel (lihat Gambar 2.5(c)). Pada level ini, lokasi pasti dari tonjolan dicatat, tetapi detail geometris dan dimensi tonjolan diabaikan. Lokasi tempat tonjolan muncul, berakhir, terbelah, atau menyatu dengan tonjolan lain disebut sebagai karakteristik tonjolan atau minutiae. Selain lokasinya, minutiae umumnya memiliki dua properti lain: arah dan jenis.



Gambar 2.9 Ada dua jenis detail yang digunakan untuk merepresentasikan detail Level 2 pada sidik jari: ujung tonjolan (dilambangkan sebagai lingkaran putih) dan percabangan tonjolan (dilambangkan sebagai kotak hitam). Sementara literatur forensik juga menyinggung jenis detail lainnya, ujung dan percabangan adalah anomali tonjolan yang paling banyak digunakan dalam sistem pengenalan sidik jari otomatis. Distribusi spasial titik detail ini pada gambar sidik jari diyakini unik untuk setiap jari.

Arah minutiae berada di sepanjang orientasi tonjolan lokal. Ada dua jenis dasar minutiae: akhir (juga disebut 'terminasi') dan bifurkasi (lihat Gambar 2.9). Dengan demikian, setiap minutiae dapat dicirikan oleh (a) lokasinya dalam gambar, (b) arah, dan (c) jenisnya. Detail level 2 dari sidik jari dapat dengan mudah diamati dalam gambar yang diperoleh pada resolusi 500 ppi. Jumlah minutiae yang ditemukan dalam sidik jari sangat bervariasi menurut metode akuisisi dan faktor-faktor lainnya. Misalnya, cetakan jari yang digulung yang ditunjukkan pada Gambar 2.3(a) memiliki 136 detail sementara cetakan polosnya pada Gambar 2.3(b) memiliki 56 detail yang diekstraksi oleh pencocok sidik jari komersial. Di sisi

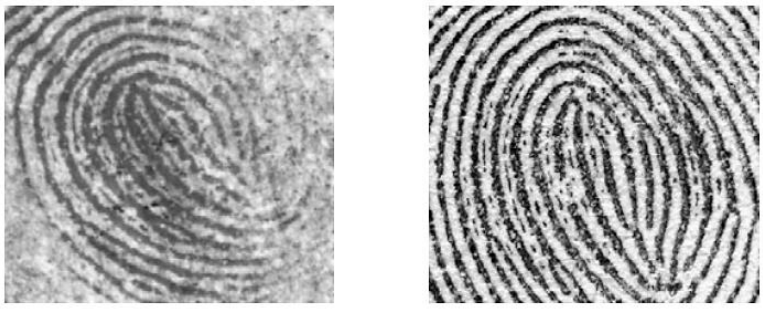
lain, hanya 18 detail yang ditemukan pada sidik jari laten pada Gambar 2.3(c) oleh pemeriksa laten.

Satu set minutiae, yang terdiri dari semua minutiae dalam sidik jari, adalah representasi abstrak dari kerangka punggungan dalam arti bahwa set minutiae menangkap sebagian besar informasi diskriminatif pada Level 2, dan kerangka punggungan dapat diturunkan secara perkiraan dari informasi minutiae saja. Representasi berbasis minutiae digunakan secara luas dalam sistem pengenalan sidik jari otomatis, terutama karena alasan berikut: (a) minutiae menangkap banyak informasi diskriminatif atau individualitas dalam sidik jari, (b) representasi berbasis minutiae adalah penyimpanan yang efisien, dan (c) ekstraksi minutiae cukup kuat terhadap berbagai sumber degradasi. Distribusi spasial minutiae dalam sidik jari adalah topik studi menarik yang telah memperoleh perhatian yang meningkat karena kebutuhan untuk menilai individualitas sidik jari menggunakan informasi minutiae saja.

Fitur Level 3

Pada level ketiga (terbaik), sidik jari direpresentasikan menggunakan lubang bagian dalam (pori-pori keringat) dan kontur luar (tepi) tonjolan. Jadi tonjolan tidak lagi dilihat sebagai gambar kerangka sederhana selebar satu piksel. Sebaliknya, informasi yang tertanam dalam tonjolan diamati secara terperinci. Tonjolan dan titik yang baru terbentuk juga disertakan pada level ini (lihat Gambar 2.5(d)). Tonjolan yang baru terbentuk adalah tonjolan yang belum matang, yang lebih tipis daripada tonjolan yang matang dan tidak mengandung pori-pori keringat. Titik adalah tonjolan yang sangat pendek yang hanya mengandung satu unit tonjolan.

Dengan kemajuan teknologi penginderaan sidik jari, banyak sensor kini dilengkapi dengan kemampuan pemindaian 1000 ppi yang dibutuhkan untuk menangkap detail Level 3 dalam sidik jari. Gambar 1.4 di Bab 1 menunjukkan gambar yang diambil pada 500 ppi dan 1000 ppi oleh pemindai optik CrossMatch L SCAN 1000P dari bagian sidik jari yang sama. Ciri-ciri Level 3 semakin banyak mendapat perhatian karena pentingnya ciri-ciri tersebut dalam mencocokkan sidik jari laten yang umumnya mengandung lebih sedikit detail daripada sidik jari yang digulung atau sidik jari biasa. Gambar 2.10(a) menunjukkan ciri-ciri Level 3 yang diekstrak dari sidik jari laten yang juga diamati pada sidik jari yang digulung (Gambar 2.10(b)).



Gambar 2.10 Fitur Level 3 yang diamati pada sidik jari laten dan sidik jari gulung yang dikawinkan.

(a) Sidik jari laten dengan pori-pori dan tonjolan yang baru terbentuk dan (b) sidik jari gulung yang dikawinkan dengan konfigurasi yang sama dengan fitur Level 3 yang diamati pada (a).

Fitur tambahan

Sidik jari sering kali memiliki fitur lain seperti lipatan, luka, dan bekas luka. Meskipun fitur-fitur ini tidak melekat pada pembentukan sidik jari, fitur-fitur ini dapat menjadi permanen tergantung pada tingkat keparahan luka dan bekas luka. Namun, karena fitur-fitur ini tidak universal seperti tiga level fitur yang dibahas sebelumnya, kegunaannya dalam pencocokan sidik jari terbatas. Faktanya, kelainan seperti itu sering kali menjadi sumber kesalahan pencocokan, seperti yang dibahas nanti.

Pembentukan

Proses pasti pembentukan pola tonjolan gesekan tidak sepenuhnya diketahui. Penelitian embriologi telah menunjukkan bahwa tonjolan epidermis didahului oleh pembentukan bantalan volar yang pertama kali muncul sekitar minggu keenam perkembangan janin. Tonjolan gesekan muncul sekitar bulan keempat kehamilan sebagai akibat dari tekanan selama pertumbuhan janin; tonjolan tidak terangkat pada kulit sampai sekitar minggu kedelapan belas. Minutiae terbentuk saat tonjolan terpisah dan menciptakan ruang untuk membentuk tonjolan baru karena pertumbuhan permukaan jari.

Aliran tonjolan pada batas jari berjalan sejajar dengan alur kuku jari dan lipatan jari. Pola aliran tonjolan di area tengah, juga disebut sebagai area pola, jari diatur oleh bentuk, ukuran, dan penempatan bantalan volar; bantalan volar yang lebih tinggi dan simetris cenderung menghasilkan lingkaran, bantalan volar yang lebih datar dan simetris cenderung menghasilkan lengkungan, dan bantalan volar asimetris cenderung menghasilkan lingkaran. Secara umum dipahami dan disetujui bahwa pola tonjolan gesekan tidak hanya dipengaruhi oleh faktor genetik tetapi juga oleh tekanan dan ketegangan fisik acak selama perkembangan janin. Efek acak ini selama morfogenesis sidik jari diyakini memberikan keunikan pada sidik jari.

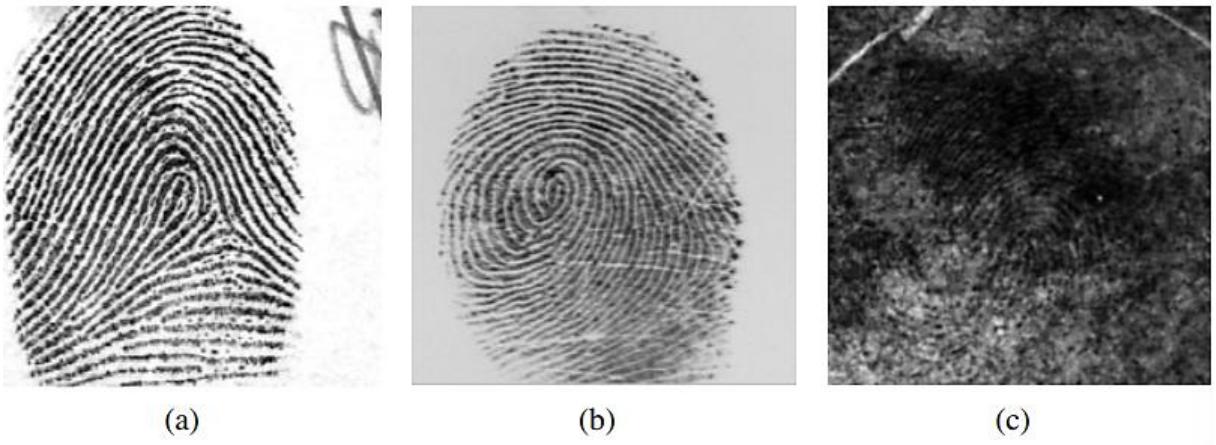
2.3 AKUISISI SIDIK JARI

Langkah pertama dalam pengenalan sidik jari adalah akuisisi gambar - proses pengambilan dan digitalisasi sidik jari seseorang untuk diproses lebih lanjut. Secara tradisional, teknik tinta di atas kertas telah digunakan untuk menangkap informasi sidik jari dari seseorang. Ini adalah teknik akuisisi dan perekaman yang sederhana - namun ampuh - yang telah digunakan sejak akhir abad ke-19. Namun, alasan utama popularitas pengenalan sidik jari, khususnya dalam aplikasi non-forensik, adalah ketersediaan sensor yang matang, praktis, dan berbiaya rendah yang dapat dengan cepat memperoleh sidik jari seseorang dengan intervensi minimal atau tanpa intervensi dari operator manusia. Sensor sidik jari yang ringkas ini juga telah tertanam di banyak perangkat konsumen seperti laptop dan ponsel. Di bawah ini, kami membahas beberapa teknik penginderaan yang telah dikembangkan untuk memperoleh sidik jari dari subjek.

Teknik penginderaan

Secara umum, citra digital sidik jari dapat diperoleh dengan menggunakan metode offline atau online (lihat Gambar 2.11). Teknik offline umumnya tidak menghasilkan citra digital langsung dari ujung jari. Sebaliknya, sidik jari pertama-tama dipindahkan ke substrat (misalnya, kertas) yang kemudian didigitalkan. Misalnya, citra sidik jari bertinta, bentuk paling umum dari penangkapan offline, diperoleh dengan terlebih dahulu mengoleskan tinta ke ujung jari subjek dan kemudian menggulung atau menekan jari pada kertas, sehingga menciptakan kesan tonjolan sidik jari pada kertas. Kesan tersebut kemudian dipindai dan didigitalkan menggunakan pemindai dokumen flatbed.

Kartu sepuluh sidik jari (lihat Gambar 2.2) yang digunakan oleh beberapa lembaga penegak hukum merekam sidik jari bertinta seseorang. Meskipun perolehan sidik jari bertinta masih dalam praktik, hal itu tidak layak dan tidak dapat diterima secara sosial dalam konteks aplikasi non-forensik. Pengembangan sidik jari laten adalah contoh lain dari metode off-line. Sidik jari laten diangkat dari permukaan benda yang disentuh atau dipegang oleh seseorang (Gambar 2.11(c)). Hal ini dicapai melalui berbagai cara mulai dari fotografi sederhana hingga pembersihan debu atau pemrosesan kimia yang lebih rumit.

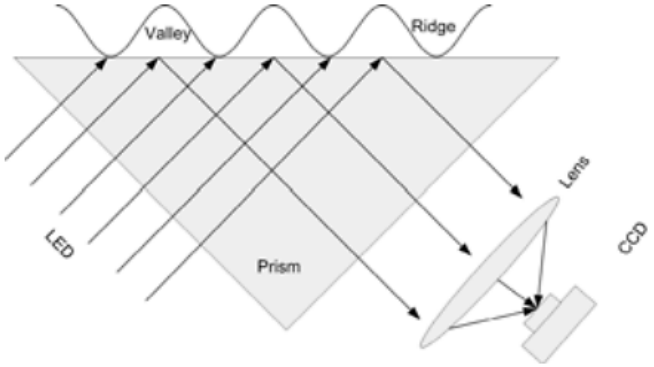


Gambar 2.11 Ada beberapa cara untuk memperoleh dan mendigitalkan sidik jari seseorang.

(a) Sidik jari dapat terlebih dahulu dipindahkan ke substrat kertas dengan meletakkan ujung jari yang bertinta secara manual di atas kertas, lalu mendigitalkan hasil cetakan menggunakan pemindai datar, (b) sidik jari hasil pemindaian langsung dapat langsung diambil citranya dari sidik jari berdasarkan sejumlah teknologi penginderaan canggih, (c) sidik jari laten dapat diambil dari objek di tempat kejadian perkara menggunakan proses kimia atau listrik.

Sebaliknya, teknik on-line menghasilkan gambar digital langsung dari ujung jari subjek melalui teknologi pencitraan digital (dijelaskan di bawah) yang menghindari kebutuhan untuk memperoleh kesan pada substrat. Gambar sidik jari yang dihasilkan disebut sebagai sidik jari pemindaian langsung. Sebagian besar sensor populer untuk memperoleh gambar sidik jari pemindaian langsung didasarkan pada teknologi optik atau kapasitif. Deskripsi singkat beberapa teknologi penginderaan pemindaian langsung disajikan di bawah ini.

(a) Optical Frustrated Total Internal Reflection (FTIR): Teknik ini menggunakan pelat kaca, sumber cahaya LED (atau laser), dan kamera CCD (atau CMOS) untuk membuat gambar sidik jari. Ketika jari diletakkan di satu sisi pelat kaca (prisma), hanya tonjolan jari yang bersentuhan dengan pelat, bukan lembah (lihat Gambar 2.12). Sistem pencitraan pada dasarnya terdiri dari rakitan sumber cahaya LED dan kamera CCD yang diletakkan di sisi lain pelat kaca. Sumber cahaya menerangi kaca pada sudut tertentu dan kamera diletakkan sedemikian rupa sehingga dapat menangkap cahaya yang dipantulkan dari kaca. Cahaya yang mengenai tonjolan tersebar secara acak (dan menghasilkan gambar gelap), sedangkan cahaya yang mengenai lembah mengalami pantulan internal total (dan menghasilkan gambar terang). Sulit untuk memiliki susunan ini dalam bentuk yang ringkas, karena panjang fokus lensa kecil bisa sangat besar. Lebih jauh, distorsi gambar mungkin terjadi ketika cahaya yang dipantulkan tidak difokuskan dengan benar.



Gambar 2.12 Penginderaan sidik jari berbasis FTIR.

(b) Kapasitansi: Sensor sidik jari live-scan solid state berbasis kapasitansi lebih umum digunakan daripada sensor FTIR optik karena ukurannya sangat kecil dan dapat dengan mudah ditanamkan ke dalam komputer laptop, ponsel, periferal komputer, dan sejenisnya. Sensor sidik jari berbasis kapasitansi pada dasarnya terdiri dari serangkaian elektroda. Dalam susunan yang umum, ada puluhan ribu pelat kapasitansi kecil (elektroda) yang tertanam dalam sebuah chip. Kulit sidik jari bertindak sebagai elektroda lainnya, sehingga membentuk kapasitor mini. Muatan listrik kecil tercipta di antara permukaan jari dan masing-masing pelat ini ketika jari diletakkan pada chip. Besarnya muatan listrik ini bergantung pada jarak antara permukaan sidik jari dan pelat kapasitansi. Dengan demikian, tonjolan dan lembah sidik jari menghasilkan pola kapasitansi yang berbeda di seluruh pelat. Kapasitansi akibat tonjolan lebih tinggi daripada yang terbentuk oleh lembah. Kapasitansi diferensial ini merupakan dasar pengoperasian sensor solid state berbasis kapasitansi. Teknik ini rentan terhadap pelepasan muatan elektrostatik dari ujung jari yang dapat memengaruhi sensor secara drastis; pentanahan yang tepat diperlukan untuk menghindari masalah ini.

(c) Pantulan Ultrasonik: Metode ultrasonik didasarkan pada pengiriman sinyal akustik ke ujung jari dan menangkap sinyal gema. Sinyal gema digunakan untuk menghitung

citra jangkauan sidik jari dan, selanjutnya, struktur tonjolan itu sendiri. Sensor memiliki dua komponen utama: pengirim, yang menghasilkan pulsa akustik pendek, dan penerima, yang mendeteksi respons yang diperoleh saat pulsa ini memantul dari permukaan sidik jari. Metode ini mengambil gambar permukaan bawah sidik jari dan, oleh karena itu, tahan terhadap kotoran dan minyak yang dapat merusak sidik jari secara visual. Akan tetapi, perangkat ini mahal, dan karenanya tidak cocok untuk produksi skala besar.

(d) Efek Piezoelektrik: Sensor yang peka terhadap tekanan telah dirancang untuk menghasilkan sinyal listrik saat tekanan mekanis diberikan padanya. Permukaan sensor terbuat dari bahan dielektrik nonkonduktor yang, saat mengalami tekanan dari jari, menghasilkan sejumlah kecil arus. (Efek ini disebut efek piezoelektrik). Kekuatan arus yang dihasilkan bergantung pada tekanan yang diberikan oleh jari pada permukaan sensor. Karena tonjolan dan lembah terdapat pada jarak (ketinggian) yang berbeda dari permukaan sensor, keduanya menghasilkan jumlah arus yang berbeda. Teknik ini tidak menangkap relief sidik jari secara akurat karena sensitivitasnya yang rendah.

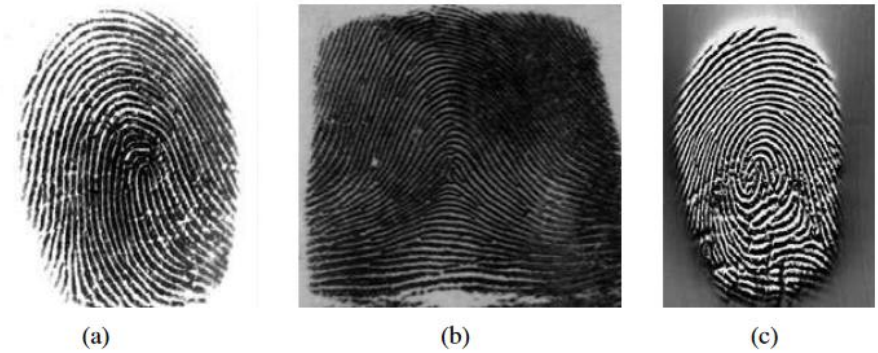
(e) Perbedaan Suhu: Sensor yang beroperasi menggunakan mekanisme ini terbuat dari bahan piro-listrik yang menghasilkan arus berdasarkan perbedaan suhu. Perbedaan suhu terjadi saat dua permukaan bersentuhan. Tonjolan sidik jari, yang bersentuhan dengan permukaan sensor, menghasilkan perbedaan suhu yang berbeda dari lembah yang jauh dari permukaan sensor. Sensor biasanya dijaga pada suhu tinggi dengan memanaskannya secara elektrik.

Kualitas gambar

Kualitas gambar sidik jari yang diperoleh memiliki dampak signifikan terhadap kinerja ekstraksi dan pencocokan fitur. Faktor penting yang menentukan kualitas sidik jari meliputi resolusi gambar, area sidik jari, dan kejelasan pola tonjolan. Dalam sebagian besar aplikasi forensik dan biometrik, resolusi gambar sebesar 500 titik per inci (ppi) diperlukan untuk pemrosesan dan pencocokan yang berhasil. Pada resolusi ini, jarak antara tonjolan yang berdekatan kira-kira 9 piksel. Badan penegak hukum kini telah mulai memindai sidik jari pada 1000 ppi untuk menangkap fitur Level 3 (lihat Gambar 1.4 di Bab 1 untuk perbandingan antara gambar sidik jari yang ditangkap pada 500 ppi dan 1000 ppi). Dalam aplikasi sipil, sensor sidik jari dengan resolusi lebih rendah dari 500 ppi sering digunakan untuk mengurangi biaya sensor.

Area sidik jari yang ditangkap dari gambar sidik jari juga merupakan faktor penting yang memengaruhi kualitas gambar. Karena bentuk jari, sidik jari biasa, yang diperoleh hanya dengan meletakkan jari pada permukaan sensor, tidak dapat menangkap seluruh sidik jari. Dalam aplikasi penegakan hukum, di mana perekaman seluruh sidik jari penting, sidik jari harus digulirkan pada permukaan sensor untuk memperoleh sidik jari penuh (ini sering kali memerlukan pemeriksa sidik jari untuk memegang jari subjek selama penggulungan). Dalam produk elektronik konsumen (misalnya, laptop dan ponsel) di mana biaya dan ukuran sensor merupakan masalah penting, sensor gesek yang dapat sesempit 3 mm telah

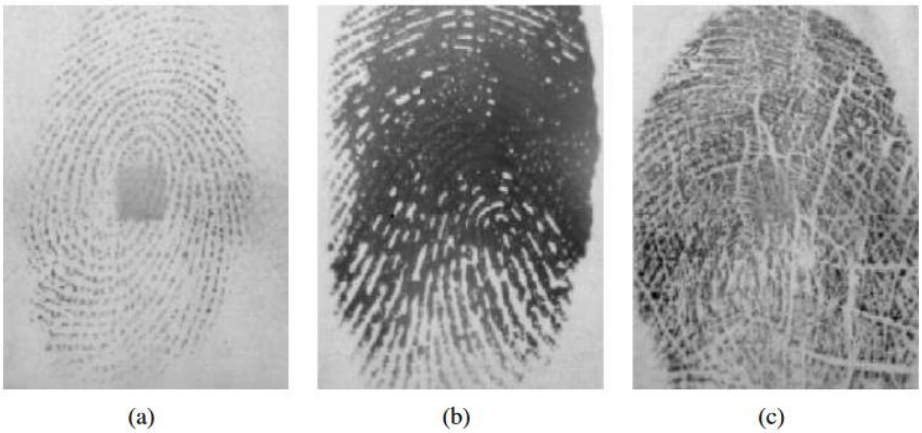
diperkenalkan. Untuk menggunakan jenis sensor ini, pengguna perlu menggesek jarinya melintasi jendela sensor, di mana semua irisan yang ditangkap digabungkan menjadi sidik jari penuh. Gambar 2.13 menunjukkan contoh sidik jari untuk masing-masing dari tiga metode operasi. Dalam aplikasi penegakan hukum di mana semua sepuluh sidik jari perlu didaftarkan, pemindai sidik jari yang dapat menangkap empat jari tangan (ibu jari ditangkap secara terpisah) atau bahkan seluruh tangan secara bersamaan lebih disukai.



Gambar 2.13 Metode pengoperasian pemindai sidik jari

(a) Sidik jari polos diperoleh dengan hanya meletakkan jari pada permukaan sensor sidik jari; (b) sidik jari gulung diperoleh dengan menggulung jari dari "paku ke kuku" pada permukaan sensor sidik jari (ini biasanya memerlukan seseorang untuk memegang jari untuk membantu menggulung dengan benar); (c) sidik jari sapuan diperoleh dengan menggabungkan irisan sidik jari yang sempit (biasanya selebar 3 mm) saat pengguna menggesekkan jarinya di sensor.

Kejelasan pola tonjolan merupakan penentu kualitas yang penting lainnya. Baik kulit jari maupun sensor memiliki dampak besar pada kejelasan tonjolan. Pada sidik jari berkualitas baik, tonjolan terus mengalir dan tonjolan yang berdekatan terpisah dengan baik. Saat jari lembap, tonjolan yang berdekatan dapat bergabung; bila kering, tonjolannya mungkin banyak yang patah; dan kualitas bawaan beberapa jari buruk (lihat Gambar 2.14). Citra sidik jari yang diperoleh menggunakan teknik pemindaian langsung atau teknik tinta biasanya memiliki kualitas yang lebih baik daripada sidik jari laten (lihat Gambar 2.11).

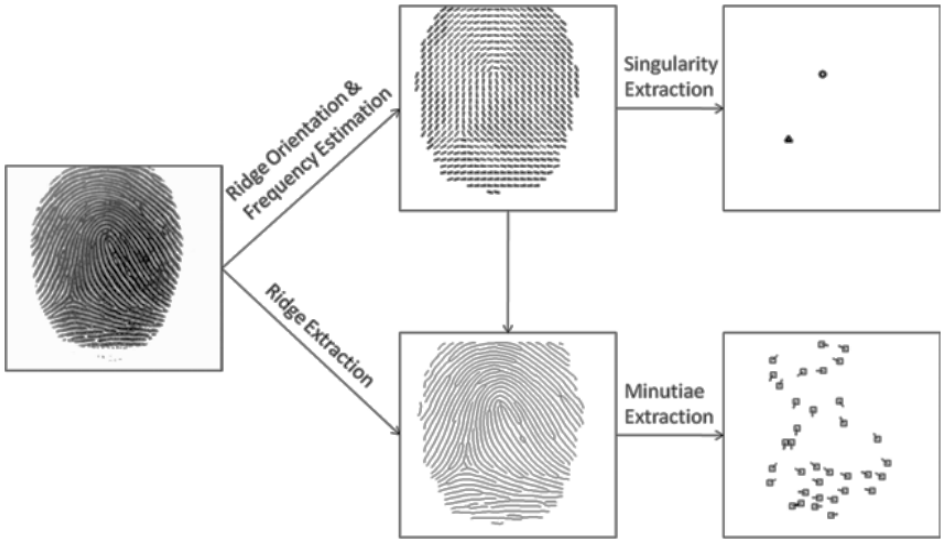


Gambar 2.14 Contoh citra sidik jari berkualitas rendah

(a) jari kering, (b) jari basah, dan (c) jari dengan banyak lipatan.

2.4 EKSTRAKSI FITUR

Sistem pengenalan sidik jari komersial sebagian besar didasarkan pada fitur Level 1 (orientasi dan frekuensi tonjolan) dan fitur Level 2 (tonjolan dan minutiae). Umumnya, fitur Level 1 diekstraksi terlebih dahulu, kemudian fitur Level 2 diekstraksi dengan panduan fitur Level 1. Gambar 2.15 menunjukkan diagram alir algoritma ekstraksi fitur umum yang mencakup empat langkah utama, yaitu (a) estimasi orientasi dan frekuensi tonjolan, (b) ekstraksi tonjolan, (c) ekstraksi singularitas, dan (d) ekstraksi minutiae. Keempat langkah utama ini dijelaskan dalam subbagian berikut.



Gambar 2.15 Diagram skema untuk ekstraksi fitur level 1 dan level 2 dari citra sidik jari

Orientasi punggungan dan estimasi frekuensi

Pola punggungan di area lokal jari dapat diperkirakan dengan gelombang kosinus

$$w(x,y) = A\cos\big(2\pi f_0(xcos\theta + ysin\theta)\big), \tag{2.1}$$

di mana A, f_0, dan θ menunjukkan amplitudo, frekuensi, dan orientasi gelombang kosinus. Maka, transformasi Fourier 2D dari gelombang kosinus diberikan oleh

$$W(u,v) = \frac{A}{2}[\delta(u - f_0\cos\theta, v\ - f_0\sin\theta) + \delta(u + f_0\cos\theta, v + f_0\sin\theta)] \tag{2.2}$$

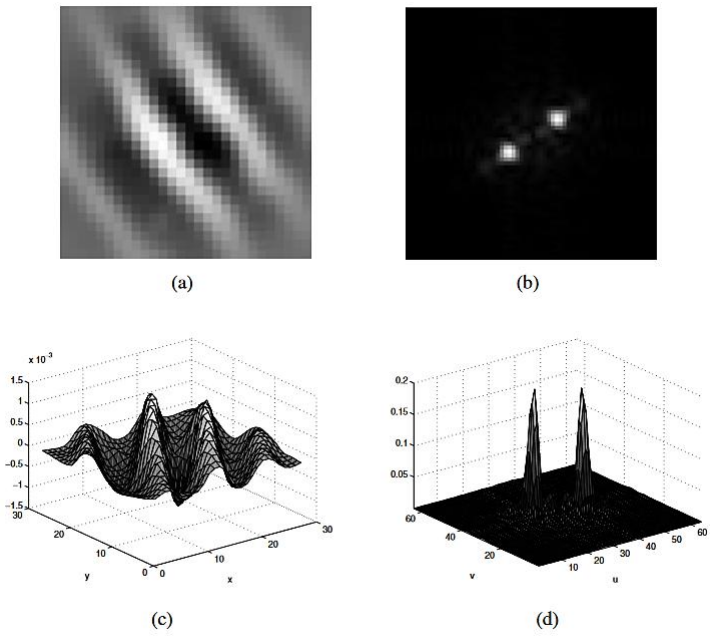
Terdiri dari sepasang impuls yang terletak pada $(f_0\cos\theta, f_0\sin\theta)$ dan $(-f_0\cos\theta, -f_0\sin\theta)$. Parameter gelombang kosinus dapat diperoleh dengan mudah dengan mendeteksi nilai maksimum spektrum magnitudo. Misalkan $(\hat{u}, \hat{v})$ menunjukkan lokasi magnitudo maksimum. Parameter gelombang kosinus diberikan oleh:

$$\hat{A} = |W(\hat{u},\hat{v})| \tag{2.3}$$

$$\widehat{\theta} = \arctan\left(\frac{\widehat{v}}{\widehat{u}}\right), \qquad \text{dan} \tag{2.4}$$

$$\widehat{f_0} = \sqrt{\widehat{u}^2 + \widehat{v}^2} \tag{2.5}$$

Karena pola punggungan lokal tidak persis gelombang kosinus, transformasi Fourier 2D-nya, yang dihitung menggunakan Fast Fourier Transform (FFT), berisi sepasang impuls kabur (lihat Gambar 2.16). Untuk memperkirakan parameter dengan lebih baik, spektrum magnitudo pertama-tama dihaluskan menggunakan filter low pass dan kemudian nilai maksimum dideteksi.



Gambar 2.16 Transformasi Fourier Diskrit (DFT) dari daerah lokal pada citra sidik jari.

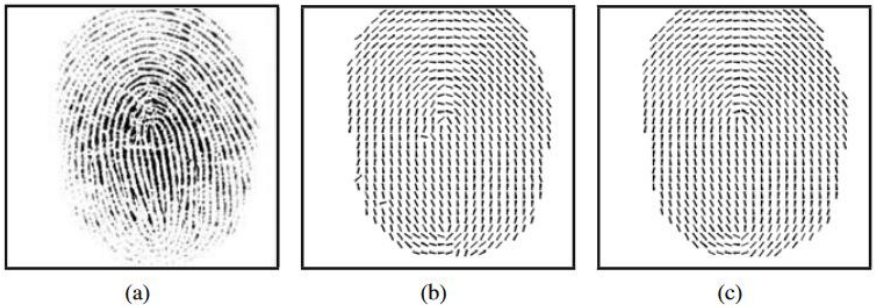
(a) Pola punggungan lokal pada sidik jari, (b) spektrum magnitudo (a), (c) pola punggungan lokal pada (a) yang ditunjukkan sebagai permukaan, dan (d) spektrum magnitudo (a) yang ditunjukkan sebagai permukaan.

Jika terdapat gangguan, seperti lipatan pada permukaan jari, estimasi awal peta orientasi punggungan dan peta frekuensi punggungan mungkin berisi wilayah lokal yang salah. Untuk memulihkan parameter pola punggungan yang benar, operasi penghalusan dengan ukuran jendela yang tepat dilakukan. Perlu dicatat bahwa meskipun peta frekuensi dapat dihaluskan menggunakan filter low pass, seperti filter Gaussian, penghalusan bidang orientasi memerlukan pertimbangan khusus. Ingat kembali bahwa orientasi punggungan sidik jari di area lokal didefinisikan dalam rentang $[0, \pi)$. Dengan demikian, sebuah vektor pada bidang 2D dengan sudut θ dan vektor lain dengan sudut $(\theta + \pi)$ berkorespondensi dengan orientasi yang sama. Akibatnya, rata-rata aritmatika sederhana dari orientasi tidak memberikan hasil yang diinginkan. Misalnya, nilai rata-rata antara 1° dan 179° seharusnya

0° dan bukan 90°. Untuk melakukan penghalusan bidang orientasi yang bermakna, prosedur tiga langkah berikut digunakan.

1. Bangun bidang vektor V = (V_x, V_y) = (cos 2 θ , sin 2 θ);
2. Lakukan penyaringan low pass pada dua komponen bidang vektor secara terpisah untuk mendapatkan bidang vektor yang dihaluskan $V^{'} = \left(V_x^{'}, V_y^{'}\right)$;
3. Medan orientasi yang dihaluskan diberikan oleh $\frac{1}{2}$ arctan $\left(\frac{V_x^{'}}{V_y^{'}}\right)$.

Gambar 2.17 menunjukkan efek penghalusan medan orientasi.



Gambar 2.17 Estimasi dan penghalusan bidang orientasi.

(a) Citra sidik jari, (b) bidang orientasi awal (berisik), dan (c) bidang orientasi yang dihaluskan.

Ekstraksi singularitas

Singularitas sidik jari dapat diekstraksi dari bidang orientasi menggunakan metode indeks Poincare yang terkenal. Indeks Poincare mengacu pada perubahan kumulatif orientasi sepanjang jalur tertutup dalam bidang orientasi. Untuk mendeteksi lokasi dan jenis singularitas secara akurat, indeks Poincare umumnya dievaluasi menggunakan delapan tetangga piksel. Misalkan $O[i] \in |0, \pi), i = 0, \ldots, 7$, menunjukkan orientasi pada delapan tetangga, yang diurutkan berlawanan arah jarum jam mulai dari tetangga mana pun, dari piksel. Indeks Poincare, PI, dari piksel dihitung sebagai

$$PI = \frac{1}{\pi}\sum_{i=0}^{7} \delta\left(O[(i+1)_{\mathrm{mod}\,8}] - O[i]\right) \tag{2.6}$$

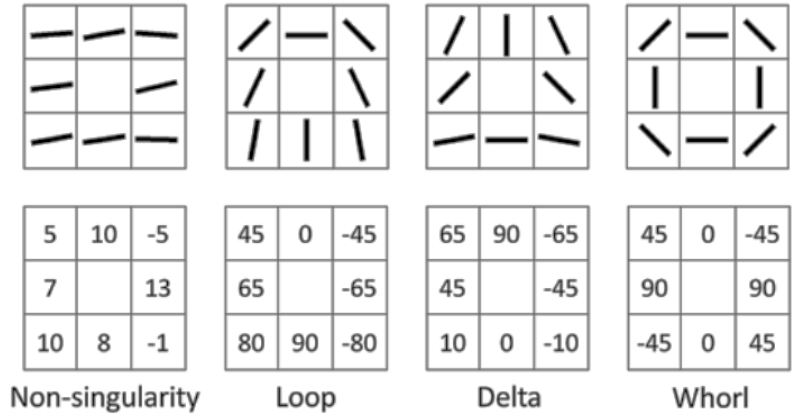
di mana $\delta(\theta)$ didefinisikan sebagai

$$\delta(\theta) = \begin{cases} \theta - \pi, \text{jika } \theta > \pi/2 \\ \theta, \text{jika } -\pi/2 \leq \theta \leq \pi/2 \\ \theta + \pi, \text{jika } \theta < -\pi/2 \end{cases} \tag{2.7}$$

Indeks Poincare untuk piksel yang sesuai dengan titik singular dapat mengambil salah satu dari empat nilai yang mungkin: 0 (non-singular), 1 (loop), -1 (delta), dan 2 (whorl). Gambar 2.18 menunjukkan contoh untuk bidang orientasi non-singular dan tiga bidang

orientasi yang berisi singularitas. Perhatikan bahwa whorl tidak didefinisikan sebagai jenis titik singular yang terpisah di Bagian 2.2 karena dapat dilihat sebagai kombinasi dari dua loop yang berdekatan yang saling berhadapan. Jelas, indeks Poincare untuk whorl sama dengan jumlah indeks Poincare dari dua loop.

Biasanya, lebih dari satu singularitas terdeteksi di sekitar singularitas sejati. Algoritma pengelompokan sederhana digunakan untuk mengelompokkan titik singular yang lokasinya berdekatan dan bertipe sama. Lokasi rata-rata sebuah kluster digunakan sebagai lokasi representatif singularitas.



Gambar 2.18 Indeks Poincare di sekitar aliran non-singular, loop, delta, dan whorl masing-masing adalah 0, 1, -1, dan 2. Baris teratas menunjukkan medan orientasi lokal dari empat kasus dan baris terbawah memberikan nilai orientasi yang sesuai dalam derajat.

Arah singularitas

Titik singular juga dapat diberi arah. Salah satu pendekatan adalah dengan mendefinisikan medan orientasi referensi untuk loop dan delta, masing-masing. Medan orientasi di sekitar titik singular sejati dapat didekati dengan versi rotasi dari medan orientasi referensi. Sudut rotasi didefinisikan sebagai arah titik singular. Medan orientasi referensi loop dan delta, masing-masing, diberikan oleh

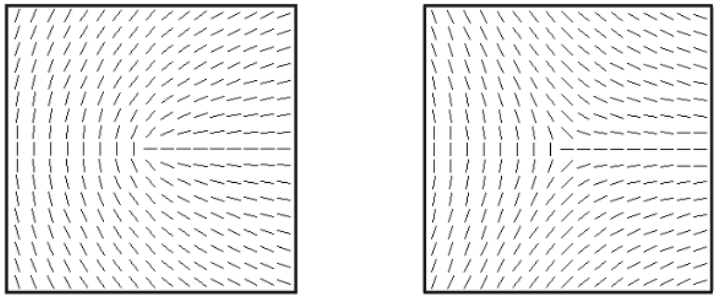
$$RO_l(x,y) = \frac{1}{2}\arctan\left(\frac{x}{y}\right) = \frac{\theta}{2}, \text{dan} \tag{2.8}$$

$$RO_d(x,y) = -\frac{1}{2}\arctan\left(\frac{x}{y}\right) = -\frac{\theta}{2} \tag{2.9}$$

di mana θ menunjukkan sudut dalam sistem koordinat kutub. Gambar 2.19 menunjukkan bidang orientasi referensi loop dan delta. Bidang orientasi referensi loop yang diputar oleh α diberikan oleh

$$RO_l(x,y;\alpha) = \frac{\theta-\alpha}{2} + \alpha = \frac{\theta}{2} + \frac{\alpha}{2} \tag{2.10}$$

Bidang orientasi referensi delta yang diputar oleh α diberikan oleh



Gambar 2.19 Bidang orientasi referensi (a) loop dan (b) delta.

$$RO_d(x,y;\alpha) = -\frac{\theta-\alpha}{2}+\alpha = -\frac{\theta}{2}+\frac{3\alpha}{2} \tag{2.11}$$

Perhatikan bahwa memutar bidang orientasi referensi delta sebesar $\alpha + n\frac{2\pi}{3}, n \in \mathbb{Z}$ (himpunan semua bilangan bulat) akan menghasilkan bidang orientasi yang sama. Selisih antara bidang orientasi lokal di sekitar singularitas dan bidang orientasi referensi diberikan oleh

$$D_{\{I,d\}}(x,y) = O(x\lambda + x_0, y\lambda + y_0) - RO_{\{I,d\}}(x,y) \tag{2.12}$$

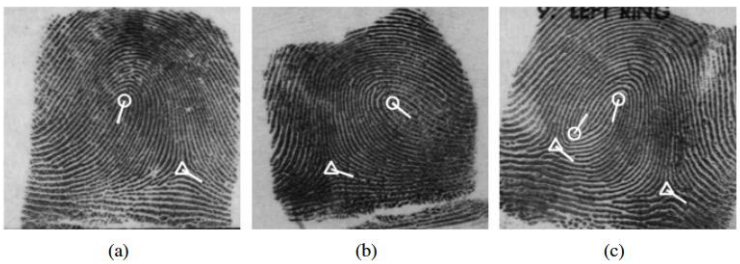
Berdasarkan persamaan (2.10), arah loop pada (x_0, y_0) dihitung dengan

$$\alpha = \arctan\left(\frac{\sum_{x=-r}^{r}\sum_{y=-r}^{r}\sin(2D_l(x,y))}{\sum_{x=-r}^{r}\sum_{y=-r}^{r}\cos(2D_l(x,y))}\right) \tag{2.13}$$

Berdasarkan persamaan (2.11), arah delta di (x_0, y_0) dihitung dengan

$$\alpha = \frac{1}{3}\arctan\left(\frac{\sum_{x=-r}^{r}\sum_{y=-r}^{r}\sin(2D_d(x,y))}{\sum_{x=-r}^{r}\sum_{y=-r}^{r}\cos(2D_d(x,y))}\right) \tag{2.14}$$

Perkiraan titik singular pada tiga sidik jari ditunjukkan pada Gambar 2.20.



Gambar 2.20 Titik singular dan arahnya.

(a) Lingkaran kiri, (b) lingkaran kanan, dan (c) lingkaran kembar.

Dengan sekumpulan titik singular dalam sidik jari yang digulung, kriteria berikut dapat digunakan untuk mengklasifikasikan sidik jari ke dalam satu dari enam jenis pola utama (seperti yang ditunjukkan pada Gambar 2.8). Perhatikan bahwa jenis lengkung dan lengkung tenda sering dimasukkan ke dalam kategori yang sama, disebut lengkung, karena kesulitan dalam membedakan antara kedua jenis ini.

1. Sidik jari diklasifikasikan ke dalam lengkung polos, jika tidak mengandung titik singular apa pun.
2. Sidik jari diklasifikasikan ke dalam lingkaran kiri, jika mengandung satu delta dan satu lingkaran yang arahnya menunjuk ke sisi kiri delta.
3. Sidik jari diklasifikasikan ke dalam lingkaran kanan, jika mengandung satu delta dan satu lingkaran yang arahnya menunjuk ke sisi kanan delta.
4. Sidik jari diklasifikasikan menjadi lengkung tenda, jika mengandung satu delta dan satu loop yang arahnya mengarah ke delta.
5. Sidik jari diklasifikasikan menjadi lingkaran, jika mengandung setidaknya dua loop dan dua delta di mana bidang orientasi punggungan di sekitar dua loop membentuk orbit melingkar.
6. Sidik jari diklasifikasikan sebagai loop kembar, jika mengandung setidaknya dua loop dan dua delta di mana bidang orientasi punggungan di sekitar dua loop tidak membentuk orbit melingkar.

Perlu dicatat bahwa keakuratan algoritma klasifikasi di atas bergantung pada keberhasilan ekstraksi singularitas, yang dapat menjadi tantangan pada sidik jari berkualitas buruk. Lebih jauh, diperlukan sidik jari yang lengkap (yaitu, sidik jari yang digulung). Oleh karena itu, jenis pola sidik jari laten yang diperoleh dari tempat kejadian perkara biasanya dianggap tidak diketahui dan sidik jari laten sering dicari berdasarkan semua jenis sidik jari dalam basis data.

Ekstraksi punggungan

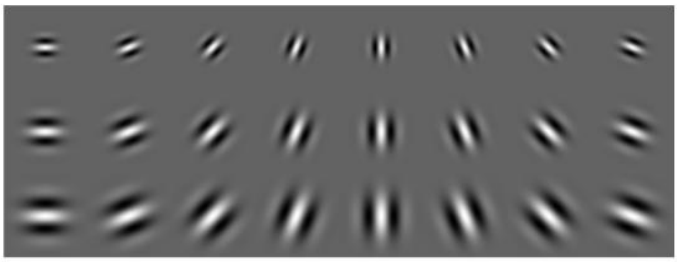
Karena minutiae merupakan titik khusus pada punggungan, wajar jika mengekstraksi punggungan terlebih dahulu lalu mendeteksi minutiae pada punggungan. Karena punggungan lebih gelap daripada lembah, metode langsung untuk mendeteksi punggungan adalah mengklasifikasikan piksel apa pun sebagai piksel punggungan jika nilai abu-abunya lebih rendah daripada ambang batas (misalnya, rata-rata lingkungan setempat).

Namun, untuk sebagian besar gambar sidik jari, metode ini tidak berfungsi dengan baik karena alasan berikut: (a) pori-pori pada punggungan lebih terang daripada piksel di sekitarnya; (b) punggungan dapat rusak karena terpotong atau terlipat; (c) punggungan yang berdekatan mungkin tampak menyatu karena kulit lembap atau tekanan. Untuk mengatasi masalah di atas, peningkatan citra sidik jari digunakan untuk menghubungkan tonjolan yang terputus dan tonjolan yang terpisah.

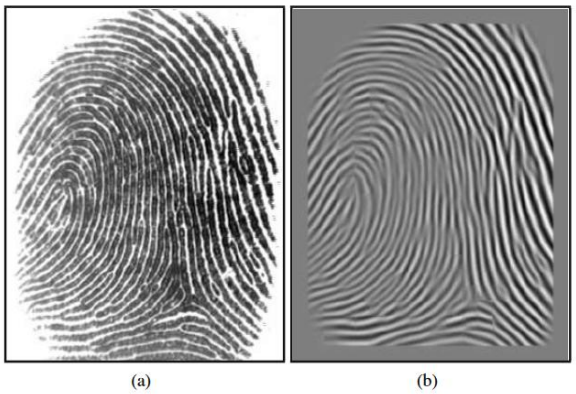
Metode peningkatan sidik jari yang berhasil didasarkan pada penyaringan kontekstual. Umumnya, ini melibatkan penyaringan citra dengan bagian riil dari filter Gabor kompleks 2D yang orientasi dan frekuensinya disesuaikan dengan orientasi dan frekuensi tonjolan lokal. Gambar 2.21 menunjukkan bagian riil dari filter Gabor 2D pada tiga skala

berbeda dan delapan orientasi berbeda. Gambar 2.22(b) menunjukkan citra yang ditingkatkan dari sidik jari pada Gambar 2.22(a).

Citra yang ditingkatkan dapat diubah menjadi citra biner dengan menggunakan ambang global (misalnya, menggunakan nilai piksel rata-rata dari citra yang ditingkatkan) atau ambang yang dihitung secara lokal. Operasi morfologi, yang disebut penipisan, digunakan untuk mengurangi lebar tonjolan menjadi satu piksel. Penipisan merupakan teknik umum dalam pemrosesan gambar, yang melibatkan penghilangan piksel-piksel di tepi luar secara berulang. Gambar 2.23 memberikan hasil langkah-langkah binerisasi dan penipisan.

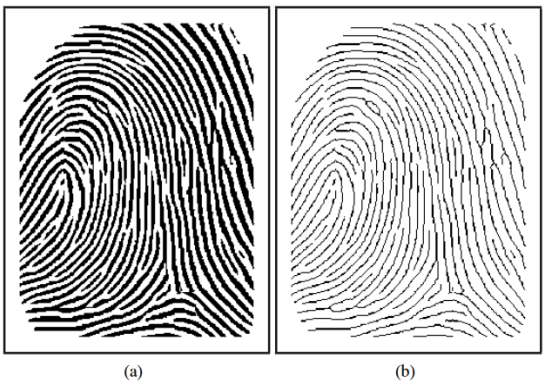


Gambar 2.21 Bagian nyata filter Gabor dengan delapan orientasi berbeda (sepanjang baris) dan tiga skala berbeda (sepanjang kolom).



Gambar 2.22 Peningkatan ridge dengan penyaringan Gabor.

(a) Citra sidik jari masukan dan (b) citra yang ditingkatkan.

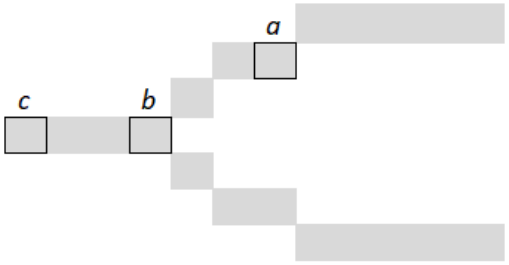


Gambar 2.23 Hasil binerisasi dan penipisan citra sidik jari pada Gambar 2.22.

(a) Citra punggungan terbinerisasi dan (b) citra punggungan yang menipis.

Ekstraksi minutiae

Setelah citra ridge yang menipis tersedia, piksel ridge dengan tiga tetangga piksel ridge diidentifikasi sebagai percabangan ridge dan piksel yang hanya memiliki satu tetangga piksel ridge diidentifikasi sebagai ujung ridge (lihat Gambar 2.24). Arah ujung ridge dihitung dengan cara berikut. Dimulai dari akhir x, kami menelusuri ridge terkait ke jarak yang tetap (misalkan 10 piksel) dan mencapai suatu titik, misalkan a. Arah xa digunakan sebagai arah minutiae. Untuk percabangan, ada tiga ridge terkait, jadi kami memperoleh tiga titik dengan menelusuri ridge ke jarak yang tetap.

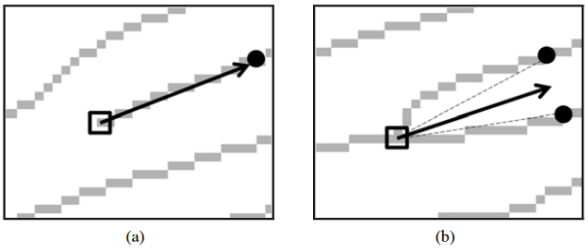


Gambar 2.24 Deteksi minutiae. Tiga jenis piksel ridge ditandai: piksel ridge tipikal 'a', percabangan ridge 'b', dan ujung ridge 'c'. Percabangan ridge atau ujung ridge mendefinisikan minutiae.

Arah percabangan didefinisikan sebagai rata-rata dari dua arah yang selisihnya paling kecil di antara ketiga ridge. Gambar 2.25 menunjukkan arah minutiae yang ditandai pada kerangka ridge. Dalam praktiknya, beberapa detail yang terdeteksi menggunakan pendekatan di atas mungkin palsu karena artefak dalam pemrosesan gambar dan gangguan dalam gambar sidik jari. Untuk menghilangkan detail palsu ini, algoritma penyaringan detail digunakan, yang biasanya terdiri dari sejumlah aturan heuristik. Misalnya, detail yang memenuhi salah satu kondisi berikut dianggap sebagai detail palsu dan dibuang:

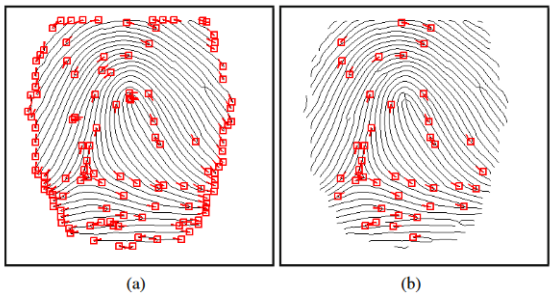
1. detail yang tidak memiliki tonjolan yang berdekatan di kedua sisi (terutama titik akhir tonjolan di sepanjang batas jari);
2. detail yang lokasinya berdekatan dan arahnya hampir berlawanan (yaitu, perbedaan antara dua arah detail mendekati 180^o);
3. terlalu banyak detail di lingkungan yang kecil.

Gambar 2.26 menunjukkan efek penyaringan detail.



Gambar 2.25 Arah minutia.

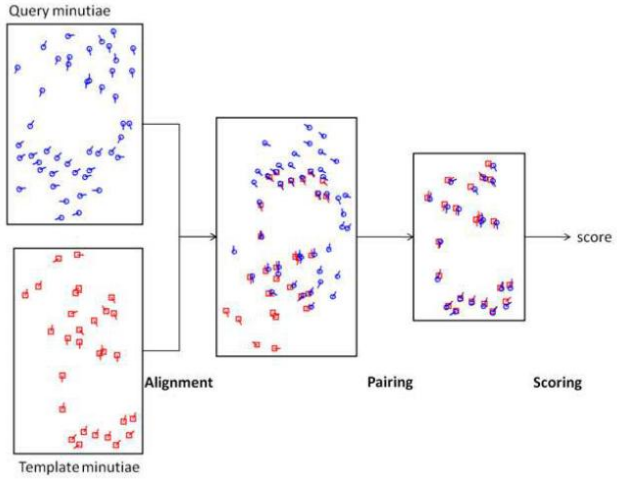
(a) Akhir punggungan dan (b) percabangan punggungan.



Gambar 2.26 Menghilangkan minutiae palsu. (a) Sebelum penyaringan minutiae dan (b) setelah penyaringan minutiae.

2.5 PENCOCOKAN

Mengingat set minutiae $\left\{x_i^Q, y_i^Q, \theta_i^Q\right\}_{i=1}^{M}$ dari sidik jari kueri dengan M minutiae dan set minutiae $\left\{x_j^T, y_j^T, \theta_j^T\right\}_{j=1}^{N}$ dari sidik jari templat dengan N minutiae, kami sekarang menjelaskan algoritma pencocokan sederhana yang terdiri dari tiga langkah (lihat Gambar 2.27):



Gambar 2.27 Diagram alir algoritma pencocokan detail.

1. Penyelarasan: Tentukan transformasi geometri antara dua set minutiae sehingga keduanya berada dalam sistem koordinat yang sama.
2. Korespondensi: Bentuk pasangan minutiae yang bersesuaian.
3. Pembuatan skor: Hitung skor kecocokan berdasarkan titik-titik minutiae yang bersesuaian.

Penjajaran

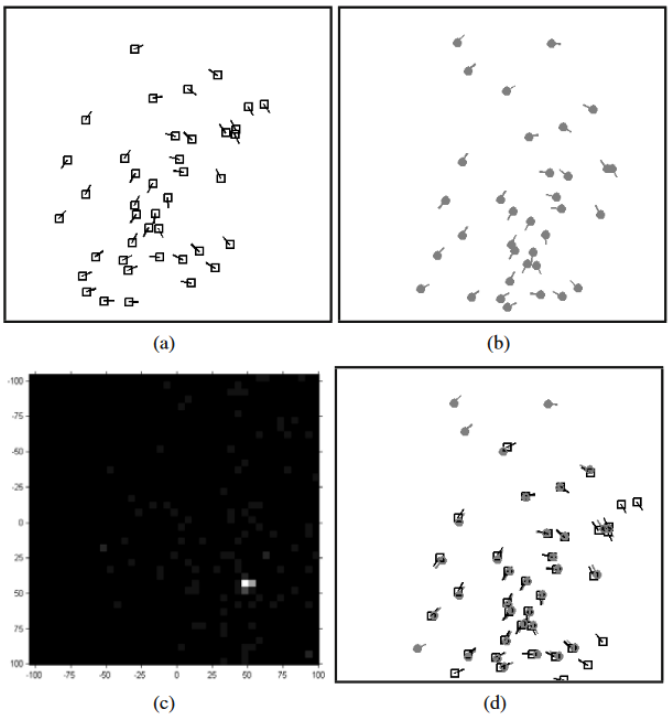
Karena dua cetakan jari yang sama yang diambil pada waktu yang berbeda dapat berbeda karena penempatan jari yang berbeda pada sensor, diperlukan proses penjajaran untuk mengubahnya ke sistem koordinat yang sama. Proses ini, yang juga dikenal sebagai registrasi, mengubah satu gambar sedemikian rupa sehingga sejajar secara geometris dengan gambar lainnya. Pertama, kita perlu menentukan model transformasi spasial. Secara

umum, transformasi kaku sudah cukup untuk pencocokan sidik jari kecuali jika terjadi deformasi nonlinier yang parah selama akuisisi sidik jari. Transformasi Hough Tergeneralisasi adalah algoritma yang terkenal untuk memperkirakan transformasi spasial antara dua set titik. Kode semu dari algoritma transformasi Hough Tergeneralisasi diberikan dalam Algoritma 1.

Gambar 2.28 mengilustrasikan pendekatan transformasi Hough untuk penyelarasan ketika hanya translasi (dalam arah x dan y) antara set minutiae kueri dan templat yang tidak diketahui. Algoritma penyelarasan sidik jari populer lainnya adalah dengan terlebih dahulu menemukan sepasang minutiae yang cocok, lalu menghitung parameter rotasi dan translasi antara dua sidik jari berdasarkan sepasang minutiae ini. Karena sifat dasar minutiae, yaitu lokasi, arah, dan jenis, tidak mengandung informasi yang cukup untuk menentukan minutiae yang cocok, informasi tambahan di sekitar minutiae perlu dikaitkan dengan setiap minutia untuk meningkatkan kekhasannya. Informasi tambahan ini disebut sebagai deskriptor minutia.

Input: atur dua set mintia $\left\{x_i^T, y_i^T, \theta_i^T\right\}_{i=1}^{M}$ dan $\left\{x_j^Q, y_j^Q, \theta_j^Q\right\}_{j=1}^{N}$
Output: Transformasikan parameter
Inisialisasi akumulator A ke 0
for $i = 1,2 \ldots, M$ **do**
    for $j = 1,2 \ldots, N$ **do**
        $\Delta\theta = \theta_i^T - \theta_j^Q$
        $\Delta x = x_i^T - x_j^Q \cos(\Delta\theta) - y_j^Q \sin(\Delta\theta)$
        $\Delta y = y_i^T - x_j^Q \sin(\Delta\theta) - y_j^Q \cos(\Delta\theta)$
        $A[\Delta\theta][\Delta x][\Delta y] = A[\Delta\theta][\Delta x][\Delta y] + 1$
    end
end
return lokasi terendah dalam A

Algoritma 1: Menentukan parameter transformasi untuk menyelaraskan dua set minutiae sidik jari menggunakan Algoritma Transformasi Hough Umum.

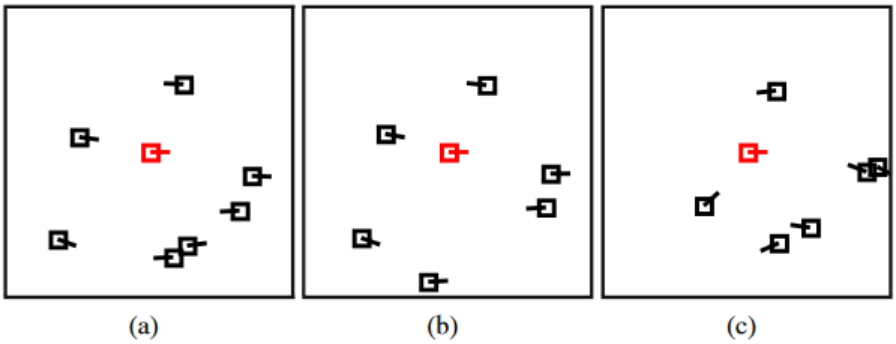


Gambar 2.28 Penyelarasan set minutiae menggunakan transformasi Hough.

(a) set minutiae kueri, (b) set minutiae templat, (c) array akumulator atau citra ruang Hough, dan (d) set minutiae yang disejajarkan. Titik "terang" dalam ruang Hough pada (c) menunjukkan sel yang menerima suara terbanyak. Translasi x dan y yang sesuai dengan sel ini digunakan untuk menyelaraskan dua set minutiae.

Deskriptor minutia yang banyak digunakan didasarkan pada himpunan minutia di sekitar minutia pusat (yaitu, minutia yang deskriptornya perlu dihitung). Lokasi dan arah minutia tetangga didefinisikan dalam sistem koordinat minutia lokal dengan menggunakan minutia pusat sebagai titik asal dan arahnya sebagai sumbu x. Dengan cara ini, deskriptor tidak berubah sehubungan dengan transformasi kaku sidik jari. Kesamaan antara dua deskriptor minutia dihitung dengan (a) pertama-tama pasangan minutia tetangga dibuat (menggunakan algoritma yang mirip dengan algoritma yang dijelaskan dalam subbagian berikutnya) dan kemudian (b) menghitung produk persentase minutia yang cocok di wilayah lokal setiap minutia sebagai berikut.

Perhatikan Gambar 2.29, di mana tiga deskriptor minutia ditampilkan; minutiae tengah pada Gambar 2.29(a) dan 2.29(b) dianggap cocok, sedangkan minutiae tengah pada Gambar 2.29(c) tidak cocok dengan minutiae pada Gambar 2.29(a) dan 2.29(b). Ada enam minutiae yang cocok (termasuk yang tengah) antara Gambar 2.29(a) dan 2.29(b), dan tiga minutiae yang cocok antara Gambar 2.29(a) dan 2.29(c). Dengan demikian, kesamaan antara minutiae pada Gambar 2.29(a) dan 2.29(b) adalah $6/8 \cdot 6/7$, lebih besar daripada kesamaan antara minutiae pada Gambar 2.29(a) dan 2.29(c), yaitu $3/8 \cdot 3/7$. Karena algoritma penyelarasan berbasis deskriptor hanya menggunakan lingkungan yang kecil, biasanya algoritma ini mengungguli algoritma transformasi Generalized Hough ketika area umum (tumpang tindih) antara dua sidik jari mengandung sangat sedikit minutiae.



Gambar 2.29 Deskriptor minutia.

(a) Deskriptor minutia (minutia sentral) pada citra sidik jari kueri, (b) deskriptor minutia pasangannya pada sidik jari templat, dan (c) deskriptor minutia lain.

Memasangkan minutiae

Setelah dua set minutiae disejajarkan, minutiae yang sesuai dipasangkan. Minutiae a dalam set minutiae templat (referensi) dikatakan berkorespondensi dengan minutiae b dalam set minutiae kueri jika dan hanya jika jaraknya berada dalam ambang batas jarak yang telah ditetapkan (misalnya, 15 piksel) dan sudut antara arahnya berada dalam ambang batas sudut lain yang telah ditetapkan (misalnya, 20 derajat).

Satu minutiae dalam sidik jari templat diizinkan untuk cocok dengan paling banyak satu minutiae dalam sidik jari kueri dan sebaliknya. Kode semu dari algoritma pemasangan minutiae diberikan dalam Algoritma 2.

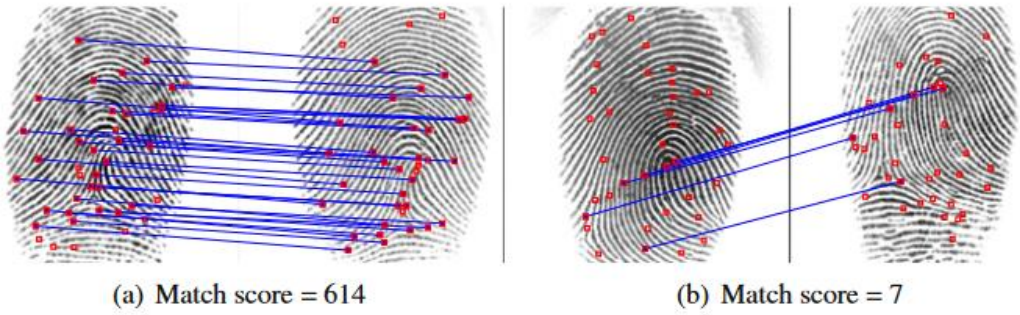
masukan: Dua set minutiae $\left\{X_i^T, y_i^T, \theta_i^T\right\}_{i=1}^{M}$ dan $\left\{X_j^Q, y_j^Q, \theta_j^Q\right\}_{j=1}^{N}$
Parameter transformasi $(\Delta\theta, \Delta x, \Delta y)$
keluaran: Daftar minutiae yang dipasangkan
Inisialisasi: set array bendera f^T, f^Q, dan jumlah sebagai 0; daftar sebagai kosong
for $i = 1,2,\cdots, M$ **do**
  for $j = 1,2,\ldots, N$ **do**
    if $f^T[i] == 0$ & $f^Q[j] == 0$ & & jarak antara minutiae i dan $j < t_d$ & rotasi di antara keduanya t_r **then**
      $f^T[i] = 1$
      $f^Q[j] = 1$
        count = count + 1
      list [count] = $\{i, j\}$
    end
  end
end
return *List*

Algoritma 2: Algoritma Pasangan Minutiae.

Pembuatan skor kecocokan

Pada langkah terakhir ini, kita perlu menghitung skor kecocokan, yang kemudian dibandingkan dengan ambang batas yang telah ditetapkan sebelumnya untuk mengklasifikasikan dua sidik jari sebagai kecocokan asli (berasal dari jari yang sama) atau kecocokan palsu (berasal dari dua jari yang berbeda). Masalah ini dapat dilihat sebagai masalah klasifikasi dua kelas dengan kecocokan asli sebagai kelas-1 dan kecocokan palsu sebagai kelas-2. Untuk masalah klasifikasi ini, beberapa fitur potensial untuk membedakan kecocokan asli dari kecocokan palsu dapat diperiksa.

Fitur pertama adalah jumlah minutiae berpasangan. Secara intuitif, kecocokan asli harus memiliki lebih banyak minutiae berpasangan daripada kecocokan palsu. Fitur berguna kedua adalah persentase minutiae yang cocok di area yang tumpang tindih antara dua sidik jari. Sekali lagi, intuitif bahwa persentase ini lebih besar untuk kecocokan asli daripada kecocokan palsu. Mengingat serangkaian hal-hal kecil, area sidik jari dapat diperkirakan dengan cangkang cembung titik-titik hal-hal kecilnya. Gambar 2.30 memperlihatkan contoh kecocokan asli dan kecocokan palsu menggunakan pencocok komersial, Neurotechnology VeriFinger SDK 4.2.

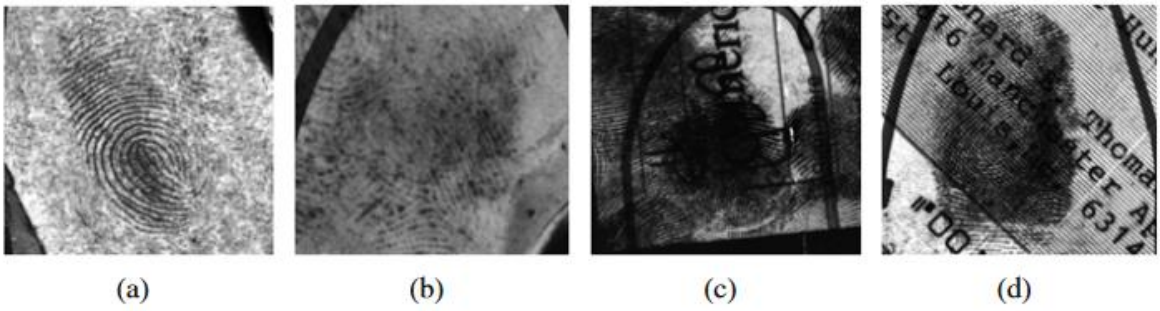


Gambar 2.30 Pencocokan sidik jari oleh pencocok komersial.

(a) Sepasang sidik jari asli dengan 31 minutiae yang cocok, dan (b) sepasang sidik jari palsu dengan 6 minutiae yang cocok. Minutiae yang sesuai antara kedua gambar dihubungkan dengan garis. Skor kecocokan dihitung sebagai beberapa fungsi dari jumlah minutiae yang cocok dan beberapa parameter lain yang merupakan hak milik pencocok komersial.

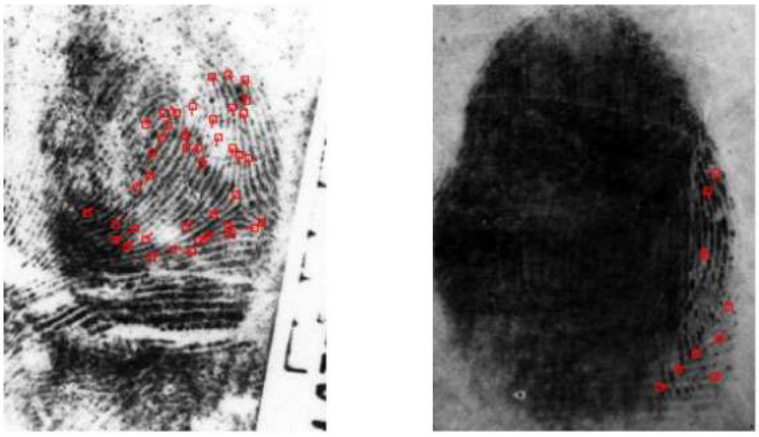
Pencocokan sidik jari laten

Pengenalan sidik jari laten sangat penting bagi lembaga penegak hukum dalam mengidentifikasi tersangka dan korban. Pencocokan sidik jari laten jauh lebih menantang daripada pencocokan sidik jari gulung atau biasa karena kualitas gambar yang biasanya buruk, area jari yang kecil, dan distorsi nonlinier yang besar pada sebagian besar laten (lihat Gambar 2.31). Ekstraktor fitur canggih tidak bekerja dengan baik untuk banyak gambar laten yang sulit. Biasanya, detail-detail kecil pada laten ditandai secara manual oleh pemeriksa laten yang terlatih untuk mengekstrak informasi terbatas yang tersedia secara efisien. Gambar 2.32 menunjukkan detail-detail kecil yang ditandai secara manual pada dua laten yang umum.



Gambar 2.31 Sidik jari laten dengan kualitas buruk.

(a) Sidik jari parsial, (b) struktur punggungan tidak jelas, (c) tumpang tindih dengan sidik jari lain, dan (d) tumpang tindih dengan latar belakang kompleks.



Gambar 2.32 Dua sidik jari laten dengan detail yang ditandai secara manual.

Karena jumlah detail kecil yang terbatas pada banyak laten, tidak mungkin untuk mencocokkan laten secara akurat hanya berdasarkan detail kecil. Sebagai contoh, sidik jari laten dalam basis data sidik jari laten domain publik, NIST SD27, memiliki 21 detail kecil per gambar sidik jari, rata-rata, (jumlah detail kecil minimum dan maksimum untuk laten dalam NIST SD27 masing-masing adalah 5 dan 82) sementara cetakan gulung yang sesuai (dipasangkan), rata-rata, memiliki 106 detail kecil (jumlah detail kecil minimum dan maksimum pada cetakan gulung dalam NIST SD27 adalah 48 dan 193).

Salah satu cara untuk meningkatkan akurasi pencocokan laten adalah dengan memanfaatkan set fitur yang lebih lengkap (yaitu, set fitur yang diperluas yang mencakup detail Level 3) dalam pencocokan. Sementara beberapa algoritme telah diusulkan untuk mencocokkan sidik jari biasa atau yang digulung menggunakan fitur yang diperluas, pencocokan laten berdasarkan fitur yang diperluas masih menjadi masalah yang terbuka. Tantangan utamanya adalah bagaimana mengodekan dan mencocokkan fitur Level 3 dengan andal dalam laten berkualitas buruk.

Individualitas sidik jari

Bukti berdasarkan sidik jari diyakini tidak dapat salah dan karenanya telah diterima di pengadilan hukum selama hampir satu abad. Namun, keandalan bukti sidik jari sedang ditantang berdasarkan standar Daubert, serangkaian kriteria mengenai penerimaan

kesaksian ilmiah yang sebagian besar berasal dari kasus Mahkamah Agung tahun 1993. Standar Daubert memiliki dua persyaratan dasar untuk sumber bukti forensik: dasar ilmiah yang mendasarinya harus diterima secara luas, dan tingkat kesalahannya harus diketahui.

Kriteria "tingkat kesalahan yang diketahui" dari aturan Daubert-lah yang terutama digunakan untuk mempertanyakan nilai ilmiah bukti sidik jari. Meskipun banyak peneliti telah mencoba memperkirakan keunikan sidik jari, masalah sebenarnya dalam memperkirakan tingkat kesalahan identifikasi sidik jari laten, yang melibatkan faktor manusia dalam banyak tahap (pengembangan laten, pengodean, pencocokan) belum terpecahkan. Satu-satunya solusi yang layak dalam waktu dekat mungkin adalah terus meningkatkan kinerja sistem sidik jari otomatis dan akhirnya mengganti pakar manusia dengan sistem otomatis.

Evaluasi kinerja

National Institute of Standards and Technology (NIST) telah melakukan beberapa evaluasi teknologi sidik jari (http://fingerprint.nist.gov), seperti *Fingerprint Vendor Technology Evaluation* (FpVTE), *Minutiae Interoperability Exchange Test* (MINEX), pengujian *Proprietary Fingerprint Template* (PFT), dan *Evaluation of Latent Fingerprint Technologies* (ELFT), yang menggunakan data operasional yang dikumpulkan dalam aplikasi forensik dan pemerintahan.

Universitas Bologna menyelenggarakan FVC-onGoing, yang merupakan evolusi dari Kompetisi Verifikasi Sidik Jari (FVC) internasional yang diselenggarakan antara tahun 2000 dan 2006. Tabel 2.1 merangkum hasil Uji Skala Menengah (MST) FpVTE 2003, FVC2006, dan ELFT 2008 (Fase II). Penting untuk dicatat bahwa kinerja sistem dapat sangat bervariasi tergantung pada karakteristik data sidik jari yang digunakan dalam evaluasi. Lebih jauh, meskipun evaluasi ini berguna, kinerja sistem biometrik yang berbeda tidak selalu dapat dibandingkan secara langsung.

Selain itu, evaluasi teknologi seperti yang dilakukan oleh NIST tidak selalu mencerminkan kinerja operasional karena perbedaan karakteristik data, lingkungan operasi, dan interaksi pengguna dengan pembaca sidik jari. Kinerja operasional sistem pengenalan sidik jari didasarkan pada beberapa faktor, termasuk karakteristik sensor, jumlah subjek dan distribusi demografis populasi yang terdaftar dalam sistem, dan berbagai faktor lingkungan, termasuk dalam ruangan versus luar ruangan, suhu, kelembaban, dan sebagainya. Selain itu, nilai FMR dan FNMR yang diperlukan bergantung pada aplikasi spesifik. Misalnya, sistem masuk berbasis sidik jari Disney World beroperasi pada FNMR rendah, agar tidak mengecewakan pelanggan yang membayar dengan menolak mereka, dengan mengorbankan FMR yang lebih tinggi.

Di sisi lain, sistem kontrol akses sidik jari dengan keamanan tinggi mungkin memerlukan FMR rendah dengan risiko FNMR yang lebih tinggi. Dalam beberapa kasus, sistem pengenalan sidik jari bahkan mungkin tidak berhasil menangkap sidik jari pengguna. Pengguna ini mungkin, misalnya, memiliki pekerjaan tertentu yang melibatkan pekerjaan manual atau orang tua dengan jari yang "usang". Dalam praktiknya, tingkat Kegagalan

Mendaftar (FTE) bisa jadi agak tinggi (hingga beberapa poin persentase) tergantung pada populasi target, karakteristik sensor, dan pekerjaan pengguna dalam populasi tersebut.

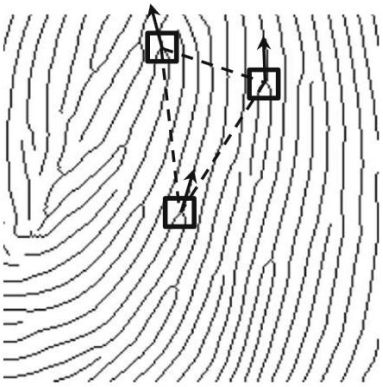
Tabel 2.1 Evaluasi kinerja teknologi sidik jari

Evaluasi	Data	Akurasi terbaik yang dilaporkan
NIST FpVTE 2003 (MST)	10.000 sidik jari polos	FNMR = 0,6% pada FMR = 0,1%
FVC2006	140 jari, 12 gambar per jari Sensor medan listrik (250 ppi) Sensor optik (569 ppi) Sensor sapuan (500 ppi)	FNMR = 15% pada FMR = 0,1% FNMR = 0,02% pada FMR = 0,1% FNMR = 3% pada FMR = 0,1%
NIST ELFT 2008 (Fase II)	835 sidik jari laten, 100.000 sidik jari yang digulung	FNMR = 8% dan FMR = 1%

2.6 PENGINDEKSAN SIDIK JARI

Selain penyelarasan dan pencocokan, titik-titik minutiae yang diekstrak dari citra sidik jari juga dapat digunakan untuk mengindeks sidik jari. Pengindeksan adalah proses pemberian nilai numerik (skalar atau vektor) pada citra sidik jari berdasarkan fitur-fitur yang diekstrak darinya. Pengindeksan sidik jari, seperti klasifikasi sidik jari, dapat digunakan untuk mempercepat proses identifikasi sidik jari dengan membandingkan citra probe input hanya dengan sebagian kecil citra dalam basis data (galeri) yang memiliki nilai indeks yang sebanding.

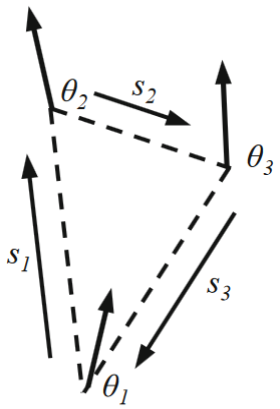
Pengindeksan berdasarkan titik-titik minutiae biasanya tidak memerlukan penyelarasan sidik jari secara eksplisit. Lebih jauh, tidak seperti skema klasifikasi sidik jari, titik-titik singular tidak perlu ada dalam citra untuk pengindeksan. Hal ini memungkinkan pengindeksan sebagian sidik jari yang berhasil. Perhatikan bahwa penangkapan sebagian sidik jari merupakan salah satu sumber utama kesalahan pencocokan.



Gambar 2.33 Triplet minutia yang terbentuk dari tiga titik minutia pada sidik jari yang dikerangkai. Sudut minutia dihitung dari arah tonjolan pada titik minutia (ditunjukkan menggunakan kepala panah).

Salah satu teknik yang paling populer untuk pengindeksan sidik jari didasarkan pada triplet minutiae (lihat Gambar 2.33). Dalam teknik ini, setiap triplet minutiae dijelaskan oleh vektor fitur sembilan dimensi yang terdiri dari sifat geometris segitiga yang dibentuk oleh triplet tersebut. Fitur-fitur tersebut meliputi panjang sisi segitiga, jumlah punggungan antara setiap pasangan titik sudut, dan orientasi titik-titik minutiae pada titik-titik sudut yang dikodekan sehubungan dengan sisi terpanjang. Fitur-fitur ini tidak berubah terhadap rotasi dan translasi. Namun, panjang sisi-sisinya sangat sensitif terhadap distorsi non-kaku. Lebih jauh, urutan fitur dan tiga sudut yang benar bergantung pada identifikasi sisi terpanjang segitiga dengan benar, seperti yang ditunjukkan pada Gambar 2.34. Sayangnya, panjang sisi-sisi segitiga tidak invarian terhadap distorsi. Algoritma pengindeksan aktual yang digunakan, bagaimanapun, didasarkan pada hashing geometris di mana prosedur kuantisasi mengatasi efek distorsi non-kaku sampai batas tertentu.

Dalam hashing geometris, semua segitiga yang diekstraksi dari sidik jari ditempatkan dalam tabel hash di mana vektor fitur yang berkaitan dengan segitiga mendefinisikan kunci dan ID sidik jari yang menghasilkan vektor fitur ini mendefinisikan nilai data. Selama pengambilan, setiap kunci dari sidik jari input digunakan untuk mengekstrak semua ID dalam tabel hash yang disimpan di bawah kunci yang sama. Akhirnya, berapa kali setiap ID diambil pada langkah sebelumnya digunakan sebagai skor kesamaan antara ID ini dan probe input.



Gambar 2.34 Set fitur yang diurutkan untuk triplet minutiae. Sisi terpanjang, S_1, muncul pertama kali dalam set fitur yang diurutkan. Demikian pula, sudut minutiae yang ditransformasikan, θ_i, dan jumlah ridge diambil dalam urutan tertentu sehubungan dengan sisi terpanjang.

Teknik ini dapat ditingkatkan dengan mengekstrak serangkaian fitur yang lebih baik dari triplet minutiae yang lebih kuat terhadap deformasi non-kaku. Di sini, vektor fitur enam dimensi terdiri dari panjang sisi terpanjang, dua sudut internal segitiga yang lebih kecil (lebih kuat terhadap distorsi dibandingkan dengan arah minutiae), kecondongan segitiga, jenisnya, dan arahnya. Dua fitur terakhir bergantung pada jenis titik minutiae yang membentuk segitiga, yaitu, percabangan punggungan atau akhir punggungan. Meskipun proses penentuan jenis minutiae (akhir punggungan atau percabangan) sensitif terhadap derau,

proses ini lebih kuat terhadap sejumlah kecil distorsi. Untuk dapat mengidentifikasi segitiga yang cocok di hadapan berbagai sumber derau, beberapa kendala geometris juga dapat diterapkan.

Selama pendaftaran, fitur sidik jari berdasarkan triplet disimpan dengan tepat dalam tabel hash. Selama pengambilan, untuk setiap triplet dalam probe input, beberapa segitiga dihasilkan dengan menerapkan fungsi distorsi pada nilai sudut. Setiap segitiga yang cocok yang ditemukan oleh pencarian ini harus secara memuaskan melewati kendala geometris yang diberlakukan oleh algoritma sebelum diterima sebagai kecocokan yang sebenarnya. Setelah menemukan segitiga yang cocok dan daftar gambar terdaftar yang sesuai, pengambilan dilanjutkan dengan mengidentifikasi kumpulan titik minutiae $M = m_1, \ldots, m_r$ yang umum antara probe input dan gambar galeri yang terdaftar.

Untuk setiap titik minutiae ini, m_1, jumlah segitiga dalam gambar yang terdaftar, i_d, yang mencakup mi dihitung. Jumlah ini diubah menjadi probabilitas posterior untuk hipotesis bahwa gambar i_d termasuk dalam identitas yang sama dengan probe yang diberikan titik minutiae umum m_1. Akhirnya, skor pengindeksan dihitung untuk setiap i_d dengan menjumlahkan n probabilitas posterior terbesar teratasnya. Gambar yang diambil diurutkan menurut skor pengindeksannya dan N gambar teratas dari basis data dikeluarkan sebagai hipotesis yang mungkin untuk dicocokkan.

2.7 SINTESIS SIDIK JARI

Sintesis sidik jari mengacu pada pembuatan citra sidik jari buatan yang mirip dengan citra sidik jari asli. Sintesis sidik jari terutama digunakan untuk membuat basis data sidik jari yang besar untuk menguji algoritme pengenalan sidik jari karena pengumpulan basis data besar citra sidik jari asli memerlukan biaya mahal baik dari segi uang maupun waktu. Tujuan lain dari sintesis sidik jari adalah untuk dapat memodelkan sidik jari dan mengidentifikasi serangkaian parameter yang tepat yang menjadi ciri sidik jari. Model yang dihasilkan, pada gilirannya, dapat membantu dalam ekstraksi dan pencocokan fitur sidik jari. Di sini, kami menyajikan algoritme sintesis sidik jari sederhana yang terdiri dari dua langkah: sintesis fitur Level 1 dan sintesis fitur Level 2.

Sintesis fitur Level 1

Fitur Level 1 berisi orientasi punggungan lokal dan frekuensi punggungan lokal. Karena variasi frekuensi ridge pada sidik jari tidak besar, biasanya frekuensi ridge tetap digunakan (0,1 ridge per piksel). Untuk tujuan sintesis bidang orientasi, sebaiknya memiliki model parametrik bidang orientasi sidik jari, yang parameternya dapat disesuaikan untuk mensimulasikan berbagai bidang orientasi. Salah satu model tersebut adalah model Zero-pole, yang parameternya adalah lokasi dan jenis titik singular:

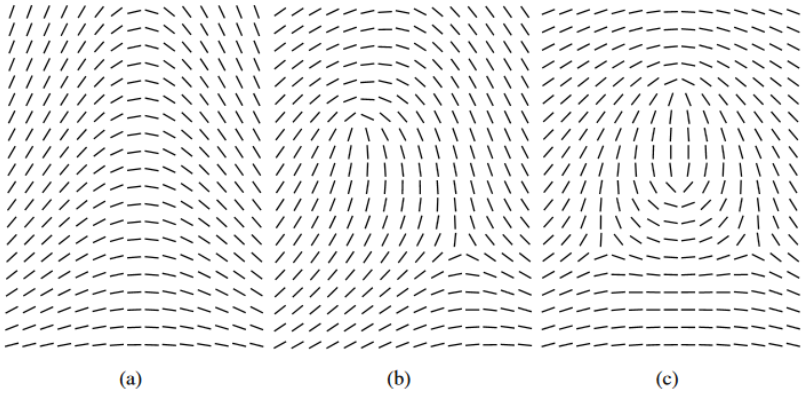
$$RO(x,y) = \frac{1}{2}\sum_{i=1}^{M} t_i \arctan\left(\frac{y-y_i}{x-x_i}\right), \qquad (2{,}15)$$

di mana M menunjukkan jumlah titik singular, (x_i, y_i) menunjukkan koordinat singularitas ke-i, dan $t_i \in \{1, -1\}$ menunjukkan jenisnya (1 untuk loop dan 1 untuk delta). Keterbatasan utama model di atas adalah tidak dapat memodelkan sidik jari tipe lengkung yang tidak memiliki singularitas dengan benar; bidang orientasi diberi nilai 0 derajat di seluruh bidang gambar.

Model yang lebih baik untuk bidang orientasi tipe lengkung diberikan oleh:

$$RO_{arch}(x, y) = \arctan\left(\left(\max\left\{0, \left(k - 3\frac{y}{H}\right)\right\} \cdot \cos\left(\frac{x}{W}\pi\right)\right)\right) \qquad (2{,}16)$$

di mana H dan W menyatakan tinggi dan lebar gambar dan $k\,(2 < k < 5)$ mengontrol kelengkungan lengkungan. Gambar 2.35 menunjukkan simulasi medan orientasi dari tiga jenis pola jari utama, yaitu lengkungan (menggunakan Persamaan (2.16)), lingkaran kiri, dan lingkaran (menggunakan Persamaan (2.15)).

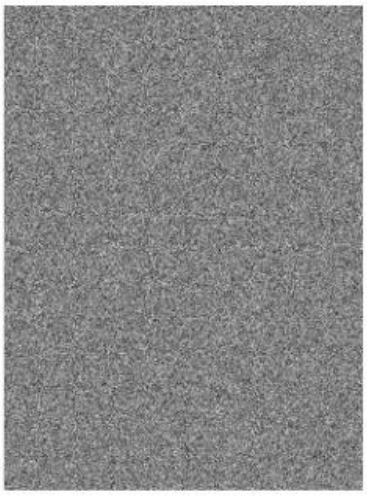


Gambar 2.35 Bidang orientasi sidik jari yang disimulasikan.

(a) Lengkungan, (b) lingkaran kiri, dan (c) lingkaran.

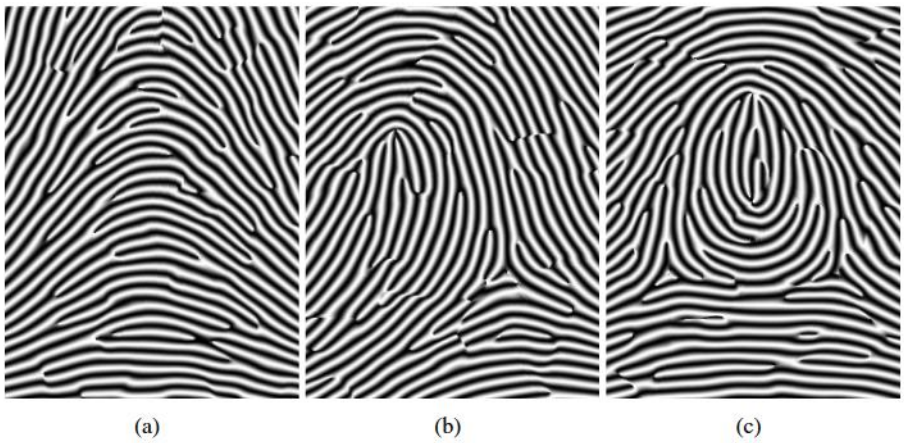
Sintesis fitur level 2

Pola punggungan dihasilkan dengan melakukan penyaringan Gabor pada gambar yang diinisialisasi dengan derau acak (lihat Gambar 2.36). Parameter penyaringan Gabor adalah bidang orientasi yang disimulasikan dan frekuensi punggungan. Derau pada setiap piksel mengikuti distribusi seragam dalam rentang [0, 255]. Gambar 2.37 menunjukkan beberapa gambar sidik jari yang disimulasikan dari lengkungan, lingkaran kiri, dan lingkaran.



Gambar 2.36 Citra noise.

Perhatikan bahwa gambar yang disintesis yang ditunjukkan pada Gambar 2.37 tampak berbeda dari gambar sidik jari yang sebenarnya. Sebagai contoh, tidak ada pori-pori keringat pada punggungan dan kontur punggungan terlalu lurus. Untuk evaluasi algoritma pencocokan sidik jari, perlu juga disimulasikan berbagai variasi intrakelas yang terkait dengan (a) ketebalan punggung telapak tangan dan kontras gambar karena faktor-faktor seperti tingkat kebasahan kulit; (b) tekanan jari pada permukaan sensor; dan (c) penempatan jari pada sensor.



Gambar 2.37 Gambar simulasi sidik jari.

(a) Lengkungan, (b) lingkaran kiri, dan (c) lingkaran.

2.8 JEJAK TELAPAK TANGAN

Pola punggung telapak tangan dan telapak kaki (lihat Gambar 2.38) juga diklaim unik dan permanen sehingga dapat digunakan untuk identifikasi pribadi. Namun, dapat dipahami bahwa jejak telapak tangan dan telapak kaki memiliki lebih sedikit aplikasi daripada sidik jari karena tidak semudah untuk menangkapnya dibandingkan dengan sidik jari. Faktanya, jejak telapak kaki hanya digunakan untuk mendaftarkan bayi baru lahir di rumah sakit karena

lebih mudah menangkap jejak telapak kaki bayi baru lahir daripada sidik jari atau sidik telapak tangan (bayi baru lahir cenderung mengepalkan tangan mereka!).

Bahkan di sana, hanya kesan bertinta dari satu-satunya cetakan yang disimpan dalam file jika ada perselisihan tentang pertukaran bayi di rumah sakit. Sidik telapak tangan mulai mendapatkan keunggulan dalam forensik untuk mengidentifikasi tersangka kejahatan dan mungkin memiliki nilai potensial dalam aplikasi sipil. Namun, lembaga penegak hukum belum memiliki basis data sidik telapak tangan yang besar yang ukurannya sebanding dengan sidik jari. Di bawah skenario Identifikasi Generasi Berikutnya (NGI) FBI, salah satu tujuan utama adalah untuk menyertakan kemampuan pencocokan sidik telapak tangan. Namun, sejauh menyangkut aplikasi forensik, manfaat utama penggunaan sidik telapak tangan adalah dalam pencocokan sidik telapak tangan laten karena diperkirakan sekitar 30% laten yang ditemukan di tempat kejadian perkara adalah telapak tangan.

Gambar 2.38 Pola tonjolan gesekan pada telapak tangan dan telapak kaki [11].

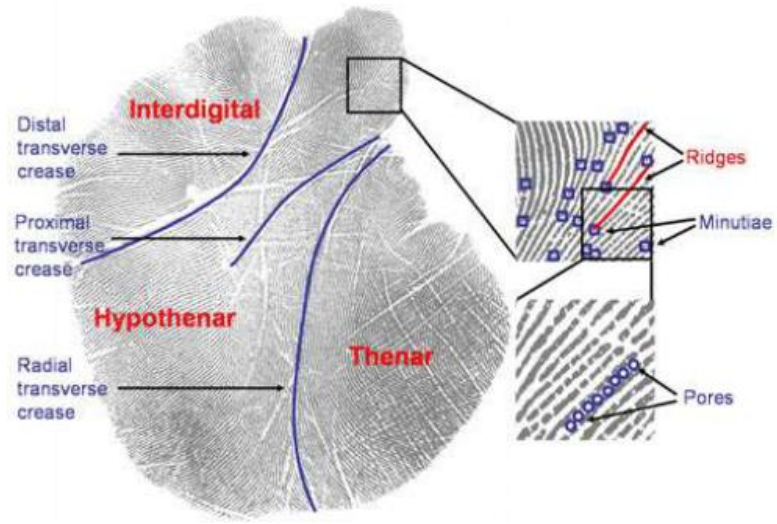
Dapat dipahami, pencocokan sidik telapak tangan lebih rumit daripada pencocokan sidik jari. Pertama-tama, dalam hal akuisisi gambar, lebih menantang untuk menangkap sidik telapak tangan daripada sidik jari karena sensornya lebih besar dan lebih mahal dan kerja sama pengguna yang lebih besar diperlukan untuk memastikan gambar sidik telapak tangan berkualitas baik karena cekungan permukaan telapak tangan.

Karena sidik telapak tangan, seperti sidik jari, juga merupakan pola punggungan gesekan, minutiae juga dapat digunakan untuk mencocokkan sidik telapak tangan. Namun, jumlah minutiae dalam sidik telapak tangan adalah urutan besarnya lebih besar daripada jumlah minutiae dalam sidik jari (sekitar 800 untuk sidik telapak tangan vs. 80 untuk sidik jari). Di bagian ini, pertama-tama kami menjelaskan fitur utama yang diamati dalam sidik telapak tangan dan kemudian memperkenalkan sistem pengenalan sidik telapak tangan dengan mempertimbangkan tantangan di atas untuk aplikasi forensik dan sipil, masing-masing.

Ciri-ciri telapak tangan

Telapak tangan terdiri dari dua ciri unik, yaitu tonjolan gesekan telapak tangan dan lipatan fleksi telapak tangan. Lipatan fleksi merupakan area perlekatan yang lebih kuat pada struktur kulit basal. Lipatan fleksi muncul sebelum pembentukan tonjolan gesekan selama tahap perkembangan kulit embrionik, dan kedua ciri ini diklaim tidak dapat diubah, permanen, dan unik bagi setiap individu. Tiga jenis utama lipatan fleksi yang paling jelas terlihat pada telapak tangan adalah: lipatan melintang distal, lipatan melintang proksimal, dan lipatan melintang radial (lihat Gambar 2.39).

Berbagai ciri pada telapak tangan dapat diamati pada resolusi gambar yang berbeda. Sementara lipatan utama dapat diamati pada resolusi kurang dari 100 ppi, lipatan tipis, tonjolan, dan hal-hal kecil hanya dapat diamati pada resolusi minimal 500 ppi; Resolusi yang jauh lebih besar dari 500 ppi diperlukan untuk mengamati pori-pori. Fitur-fitur ini ditandai pada contoh telapak tangan pada Gambar 2.39.



Gambar 2.39 Daerah (interdigital, tenar, dan hipotenar), lipatan utama (lipatan melintang distal, lipatan melintang proksimal, dan lipatan melintang radial), tonjolan, minutiae, dan pori-pori pada telapak tangan.

Pengenalan telapak tangan dalam forensik

Hingga saat ini, penggunaan utama pengenalan telapak tangan adalah untuk mengidentifikasi tersangka dengan mencocokkan telapak tangan laten yang diambil dari tempat kejadian perkara dengan basis data telapak tangan penegak hukum. Untuk mencapai akurasi tinggi, minutiae merupakan fitur utama yang digunakan dalam pencocokan telapak tangan laten, yang mengharuskan telapak tangan diambil pada resolusi 500 ppi atau lebih tinggi.

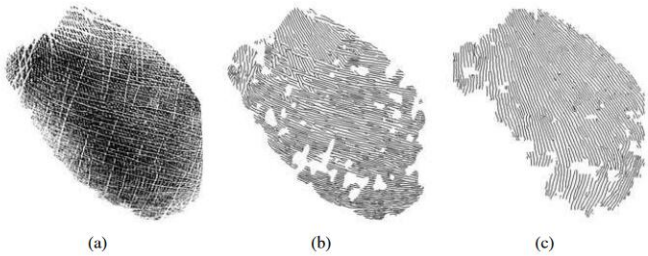
Seperti yang ditunjukkan sebelumnya, karena ukuran area telapak tangan yang besar, jumlah minutiae dalam telapak tangan kira-kira sepuluh kali lipat jumlah minutiae dalam sidik jari yang digulung. Karena kompleksitas komputasi inilah pencocokan telapak tangan penuh dengan telapak tangan penuh jarang dilakukan, terutama ketika pencocokan sepuluh

(jari) memberikan akurasi yang cukup dalam forensik, penegakan hukum, dan aplikasi penyeberangan perbatasan. Karena tekstur telapak tangan beresolusi tinggi sangat mirip dengan sidik jari, banyak teknik ekstraksi dan pencocokan detail untuk sidik jari dapat langsung diterapkan pada telapak tangan.

Namun, ada satu perbedaan utama antara telapak tangan dan sidik jari, yaitu adanya sejumlah besar lipatan pada telapak tangan. Karena lipatan ini, algoritma estimasi bidang orientasi punggungan untuk sidik jari tidak bekerja dengan baik. Algoritma estimasi bidang orientasi yang dimodifikasi untuk menangani lipatan pada telapak tangan terdiri dari langkah-langkah berikut:

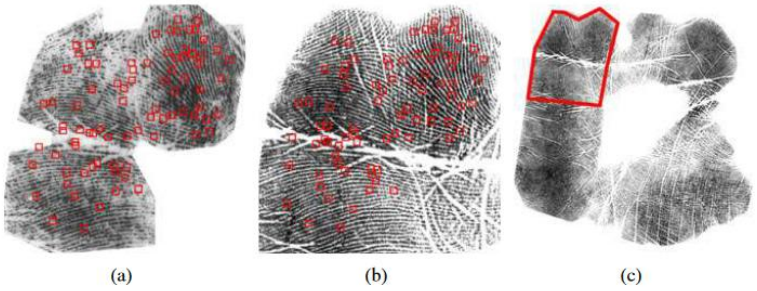
1. Mendeteksi sekumpulan enam gelombang sinusoid terkuat dalam transformasi Fourier dari setiap blok lokal (16 x 16 piksel) pada telapak tangan.
2. Mengelompokkan gelombang terkuat yang kompatibel satu sama lain ke dalam sekumpulan bidang orientasi benih. Dua gelombang di blok yang berdekatan dikatakan kompatibel jika orientasi dan frekuensinya serupa.
3. Mengembangkan setiap bidang orientasi benih dengan menyertakan gelombang yang berdekatan dan kompatibel.
4. Memilih benih terbesar sebagai bidang orientasi akhir.

Setelah bidang orientasi diperoleh, langkah-langkah ekstraksi fitur sidik jari, termasuk penyaringan Gabor, binerisasi, penipisan, dan ekstraksi minutiae, dapat langsung digunakan untuk pemrosesan dan pencocokan telapak tangan. Seperti yang ditunjukkan pada Gambar 2.40, algoritma estimasi bidang orientasi yang dimodifikasi ini menghasilkan citra kerangka punggungan yang lebih baik dibandingkan dengan kerangka punggungan yang diperoleh dari algoritma ekstraksi fitur sidik jari yang canggih. Gambar 2.41 menunjukkan contoh pencocokan telapak tangan laten yang berhasil.



Gambar 2.40 Perbandingan dua algoritma ekstraksi fitur pada telapak tangan.

(a) Sebagian telapak tangan hasil pemindaian langsung dari daerah thenar. (b) Citra kerangka punggungan (a) yang diperoleh menggunakan algoritma ekstraksi fitur sidik jari yang canggih. (c) Citra kerangka punggungan (a) yang diperoleh menggunakan algoritma ekstraksi fitur telapak tangan yang dijelaskan sebelumnya.



Gambar 2.41 Pencocokan telapak tangan laten.

(a) Telapak tangan laten dengan minutiae, (b) daerah yang sesuai pada telapak tangan yang dikawinkan, dan (c) telapak tangan penuh yang dikawinkan.

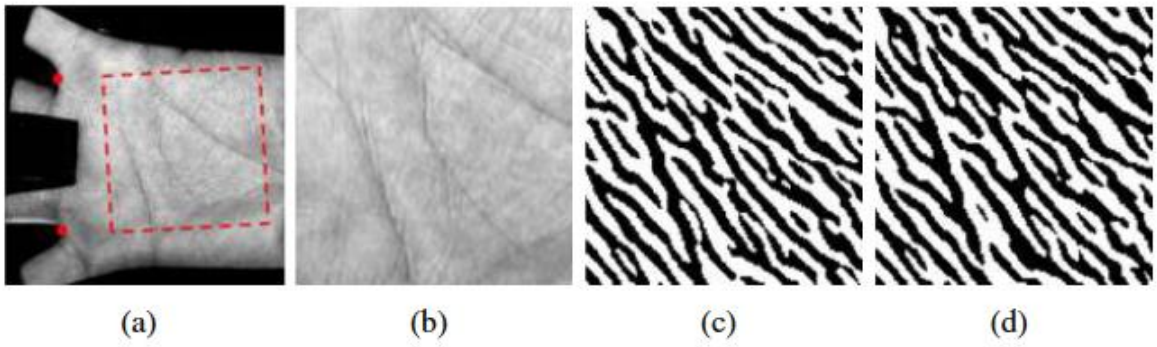
Pengenalan sidik telapak tangan untuk kontrol akses

Sistem pengenalan sidik telapak tangan dalam forensik memerlukan gambar beresolusi tinggi (setidaknya 500 ppi), sehingga menggunakan pemindai yang mahal dan memiliki kompleksitas komputasi yang tinggi. Untuk mengurangi kompleksitas komputasi dan biaya pemindai sidik telapak tangan, yang merupakan masalah penting dalam penerapan teknologi biometrik dalam aplikasi sipil (misalnya, kontrol akses), beberapa upaya telah dilakukan untuk merancang sistem pengenalan sidik telapak tangan waktu nyata yang didasarkan pada gambar beresolusi rendah (sekitar 75 ppi). Sistem ini menangkap sidik telapak tangan secara langsung menggunakan kamera digital seperti kamera web. Gambar 2.42 menunjukkan gambar sidik telapak tangan beresolusi rendah. Perhatikan bahwa tonjolan dan detail tidak terlihat jelas pada resolusi rendah ini.

Gambar 2.42 Gambar telapak tangan beresolusi rendah (75 ppi) dari basis data telapak tangan PolyU.

Oleh karena itu, sistem pencocokan sidik telapak tangan beresolusi rendah terutama didasarkan pada lipatan lengkung yang masih terlihat. Sistem pengenalan telapak tangan beresolusi rendah mengadopsi kerangka kerja pemrosesan yang mencakup (a) pemotongan dan normalisasi telapak tangan berdasarkan pendeteksian dua celah jari, (b) pemfilteran gambar yang dipotong menggunakan filter Gabor 2D dengan arah dan frekuensi yang telah ditentukan sebelumnya, dan (c) binerisasi gambar nyata dan imajiner. Proses pengodean telapak tangan ini ditunjukkan pada Gambar 2.43.

Untuk menghitung kesamaan antara dua telapak tangan, jarak Hamming antara gambar latar depan (wilayah yang diminati) nyata dan imajiner yang difilter biner dari dua telapak tangan dihitung dan dibagi dengan jumlah piksel latar depan. Untuk memperhitungkan varians kecil dalam langkah normalisasi, gambar templat biasanya diputar dan diterjemahkan untuk mendapatkan beberapa versinya yang berbeda. Jarak minimum antara gambar kueri dan semua versi gambar templat dipilih sebagai jarak akhir. Meskipun keakuratan yang dilaporkan dari sistem pencocokan sidik telapak tangan resolusi rendah sangat mengesankan, namun sistem tersebut belum terbukti kompetitif dibandingkan dengan sistem pencocokan sidik jari untuk kontrol akses atau aplikasi sipil lainnya.



Gambar 2.43 Pengodean telapak tangan.

(a) Citra telapak tangan asli yang menunjukkan wilayah yang diinginkan dan dua posisi celah jari yang digunakan untuk normalisasi, (b) citra yang dipotong, (c) citra yang difilter dan dibinerisasi oleh bagian riil filter Gabor, dan (d) citra yang difilter dan dibinerisasi oleh bagian imajiner filter Gabor.

Ringkasan

Pengenalan sidik jari adalah salah satu teknologi biometrik yang paling matang dan telah digunakan selama lebih dari 100 tahun. Meskipun teknologi sidik jari sudah matang, adopsi yang luas dalam serangkaian aplikasi yang beragam telah menimbulkan beberapa tantangan baru yang saat ini sedang ditangani oleh komunitas ilmiah.

1. Meskipun berbagai jenis teknologi penginderaan sidik jari telah dikembangkan, menangkap citra sidik jari berkualitas tinggi dari jari-jari dalam kondisi yang tidak ideal dan pengguna yang belum terbiasa masih bermasalah. Salah satu teknologi yang menjanjikan adalah akuisisi sidik jari 3D dalam mode tanpa sentuhan. Keuntungan utama dari modalitas ini adalah dapat menangkap gambar sidik jari yang

setara dengan yang digulung jauh lebih cepat daripada proses penggulungan konvensional. Hal ini juga dapat menghindari distorsi kulit yang disebabkan oleh penggulungan dan variasi tekanan lainnya.

2. Penerapan sistem pengenalan sidik jari secara luas dalam berbagai aplikasi juga telah menghasilkan beberapa metode baru untuk penghindaran. Telah dilaporkan bahwa beberapa individu telah berhasil mengalahkan sistem pengenalan positif (misalnya, sistem kontrol akses fisik) menggunakan jari palsu dan beberapa individu telah berhasil menghindari sistem pengenalan negatif (misalnya, sistem kontrol perbatasan) dengan mengubah sidik jari mereka secara bedah. Penelitian lebih lanjut diperlukan untuk memastikan integritas sidik jari yang disajikan pada sensor.
3. Meskipun pengenalan sidik jari merupakan salah satu aplikasi paling awal dari pengenalan pola, keakuratan sistem pencocokan sidik jari yang canggih masih belum sebanding dengan ahli sidik jari manusia dalam banyak situasi, khususnya pencocokan sidik jari laten yang kualitas gambarnya cenderung buruk. Sistem identifikasi sidik jari yang canggih memerlukan intervensi manual yang ekstensif dalam pengkodean laten dan dalam memverifikasi daftar kandidat yang dikembalikan oleh sistem. Dengan meningkatnya transaksi pencocokan laten untuk aplikasi sipil, penegakan hukum, dan keamanan dalam negeri, pemrosesan dan pencocokan laten otomatis merupakan bidang penelitian yang bermanfaat.
4. Penggunaan sistem pengenalan sidik jari secara luas dalam aplikasi pemerintah dan sipil berskala besar telah menimbulkan kekhawatiran tentang keamanan pola sidik jari dan privasi pengguna yang diakibatkannya. Keamanan dan privasi menjadi perhatian khusus dalam basis data terpusat, yang dapat menyimpan jutaan pola sidik jari. Teknologi yang meningkatkan privasi, bersama dengan biometrik yang dapat dibatalkan, kemungkinan akan meningkatkan tingkat privasi dan keamanan informasi pribadi yang penting tersebut. Namun, diperlukan lebih banyak penelitian untuk menggabungkan skema ini dalam lingkungan operasional.

BAB 3
PENGENALAN WAJAH

"Untuk menanyakan bagaimana manusia melakukan identifikasi wajah mungkin merupakan pertanyaan yang sulit saat ini. Namun untuk menanyakan seberapa baik dan dengan isyarat apa identifikasi dapat terjadi memang merupakan pertanyaan yang mudah. Begitu pula dengan masalah mencapai identifikasi dan pengambilan data mesin yang efektif."

Goldstein, Harmon dan Lesk, Prosiding IEEE, Mei 1971.

Gambar wajah manusia tidak hanya berguna untuk pengenalan orang, tetapi juga untuk mengungkapkan atribut lain seperti jenis kelamin, usia, etnis, dan keadaan emosional seseorang. Oleh karena itu, wajah merupakan pengidentifikasi biometrik yang penting dalam penegakan hukum dan komunitas interaksi manusia-komputer (HCI). Mendeteksi wajah dalam gambar tertentu dan mengenali orang berdasarkan gambar wajah mereka adalah masalah pengenalan objek klasik yang telah mendapat perhatian luas dalam literatur visi komputer.

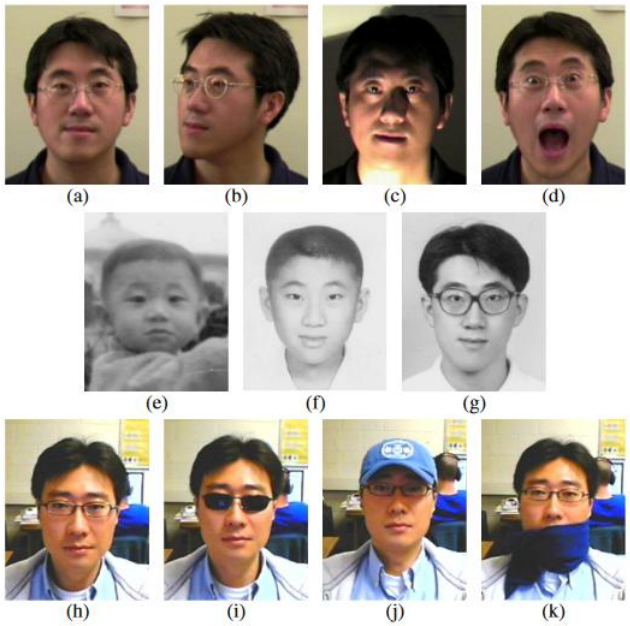
Sementara manusia dianggap pandai mengenali wajah yang dikenal, proses kognitif yang tepat yang terlibat dalam aktivitas ini tidak dipahami dengan baik. Oleh karena itu, melatih mesin untuk mengenali wajah seperti halnya manusia merupakan tugas yang sulit. Akan tetapi, metode umum yang digunakan dalam pengenalan objek seperti pendekatan berbasis tampilan, berbasis model, dan berbasis tekstur juga berlaku untuk masalah khusus deteksi dan pengenalan wajah. Bab ini memberikan gambaran umum tentang metode yang telah dikembangkan untuk pengenalan wajah otomatis dan membahas beberapa tantangan yang dihadapi oleh sistem ini.

3.1 PENDAHULUAN

Wajah adalah bagian depan kepala manusia, yang memanjang dari dahi hingga dagu dan meliputi mulut, hidung, pipi, dan mata. Sebagai bagian terpenting dalam interaksi seseorang dengan dunia luar, wajah menampung sebagian besar organ sensorik mendasar yang diperlukan untuk memahami dunia sekitar, yaitu mata untuk melihat, hidung untuk mencium, mulut untuk mengecap, dan telinga untuk mendengar. Wajah dianggap sebagai ciri biometrik yang paling umum digunakan oleh manusia; kita saling mengenali dan, dalam banyak kasus, menetapkan identitas kita berdasarkan wajah. Oleh karena itu, sudah menjadi praktik standar untuk menyertakan foto wajah dalam berbagai token autentikasi seperti kartu identitas, paspor, dan SIM.

Pengenalan wajah dapat didefinisikan sebagai proses menetapkan identitas seseorang berdasarkan karakteristik wajah mereka. Dalam bentuknya yang paling sederhana, masalah pengenalan wajah melibatkan membandingkan dua gambar wajah dan menentukan apakah mereka adalah orang yang sama. Sementara manusia tampaknya mahir dalam menentukan kesamaan antara dua gambar wajah yang diperoleh dalam kondisi yang beragam, proses pengenalan wajah otomatis dipenuhi dengan beberapa tantangan. Gambar

wajah seseorang mungkin memiliki variasi dalam usia, pose, pencahayaan, dan ekspresi wajah (lihat Gambar 3.1) serta menunjukkan perubahan dalam penampilan karena riasan, rambut wajah, atau aksesori (misalnya, kacamata hitam).



Gambar 3.1 Masalah variasi intra-kelas (yaitu, intra-pengguna) cukup jelas dalam konteks pengenalan wajah.

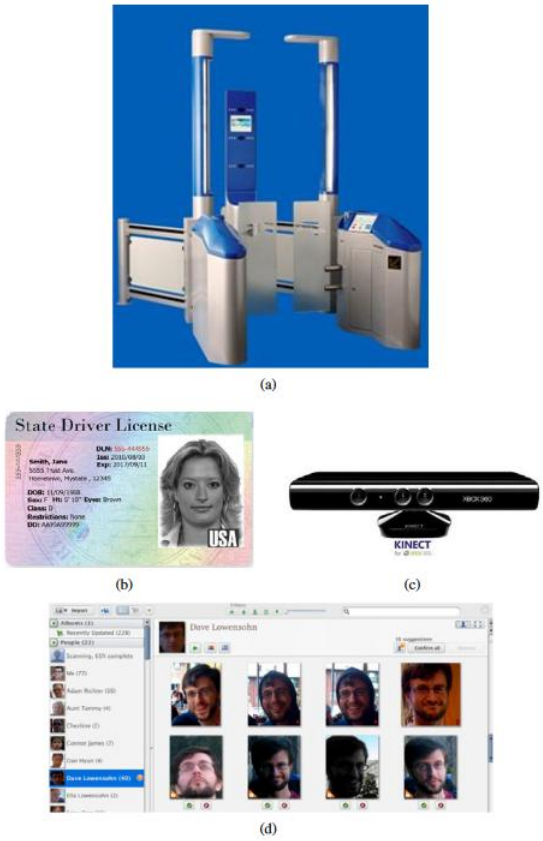
Melatih mesin untuk mengenali gambar wajah yang menunjukkan variasi intra-pengguna yang tidak dibatasi adalah tugas yang sulit, terutama karena proses kognitif dan saraf yang tepat yang terlibat dalam manusia untuk tugas pengenalan wajah (dan ingatan) masih belum sepenuhnya diketahui. Selain itu, mungkin ada kemiripan antara citra wajah orang yang berbeda (lihat Gambar 3.2), terutama jika mereka memiliki hubungan genetik (misalnya, saudara kembar identik, ayah dan anak, dll.). Kesamaan antarkelas tersebut semakin memperparah kesulitan mengenali orang berdasarkan wajah mereka. Meskipun ada tantangan ini, kemajuan signifikan telah dibuat di bidang pengenalan wajah otomatis selama dua dekade terakhir. Teknik untuk pengenalan wajah otomatis telah dikembangkan untuk tujuan pengenalan orang dari gambar diam 2 dimensi (2D), video (urutan gambar 2D), dan gambar rentang (kedalaman) 3D.

Modalitas wajah memiliki beberapa keunggulan yang membuatnya lebih disukai dalam banyak aplikasi biometrik. Pertama, tidak seperti sidik jari, wajah dapat ditangkap pada jarak yang lebih jauh menggunakan sensor nonkontak. Oleh karena itu, wajah merupakan pengenal biometrik yang cocok dalam aplikasi pengawasan. Kedua, wajah tidak hanya menyampaikan identitas, tetapi juga emosi seseorang (misalnya, kebahagiaan atau kemarahan) serta informasi biografis (misalnya, jenis kelamin, etnis, dan usia). Pengenalan wajah dan emosi terkait secara otomatis diperlukan untuk merancang antarmuka manusia-komputer yang interaktif.

(a) Twin[1] (b) Family[2]

Gambar 3.2 Masalah kesamaan antarkelas. Citra wajah beberapa orang (misalnya, saudara kembar atau keluarga) menunjukkan kemiripan dalam penampilan yang dapat membingungkan sistem pengenalan wajah otomatis.

Ketiga, ada basis data wajah lama yang besar (misalnya, repositori SIM AS mencakup lebih dari 95% populasi orang dewasa), yang memungkinkan analisis skala besar dari modalitas wajah dalam hal individualitas atau skalabilitas. Akhirnya, dibandingkan dengan ciri biometrik lainnya seperti sidik jari dan iris, orang pada umumnya lebih bersedia untuk berbagi gambar wajah mereka di domain publik sebagaimana dibuktikan oleh meningkatnya minat pada aplikasi media sosial (misalnya, Facebook) dengan fungsi seperti penandaan wajah. Karena alasan di atas, pengenalan wajah memiliki berbagai aplikasi dalam penegakan hukum, identifikasi sipil, sistem pengawasan, dan sistem hiburan/hiburan. Gambar 3.3 menggambarkan beberapa aplikasi pengenalan wajah ini.



(a) (b) (c) (d)

Gambar 3.3 Aplikasi pengenalan wajah otomatis

(a) Sistem SmartGate Australia yang memfasilitasi pengurusan imigrasi yang lebih cepat bagi pelancong terdaftar; (b) Solusi SIM Morpho, yang memungkinkan pengenalan wajah digunakan untuk mencegah satu orang memperoleh beberapa SIM dengan nama berbeda; (c) Perangkat Kinect Microsoft memiliki kemampuan

pengenalan wajah untuk tujuan personalisasi sistem permainan XBOX 360 berdasarkan identitas pemain; dan (d) Picasa Google dan situs web jejaring sosial lainnya menawarkan fungsi penandaan wajah otomatis untuk memudahkan pengelolaan album foto pribadi.

Psikologi pengenalan wajah

Penelitian di bidang psikologi dan neurokognisi menunjukkan bahwa bagian-bagian tertentu dari otak diarahkan untuk mengamati wajah. Eksperimen telah menunjukkan bahwa manusia merasa sulit untuk mendeteksi atau mengenali wajah yang terbalik meskipun mereka dapat melihat objek terbalik lainnya dengan cukup mudah. Analisis terhadap pasien yang menderita prosopagnosia (gangguan di mana seseorang kehilangan kemampuannya untuk mengenali wajah namun tetap mempertahankan kemampuannya untuk mengenali objek non-wajah lainnya) telah menunjukkan bahwa hilangnya kemampuan pengenalan wajah disebabkan oleh lesi di area otak yang disebut korteks temporal. Hal ini juga didukung oleh penelitian terpisah yang mencatat respons aktif di area korteks temporal otak monyet saat diperlihatkan gambar wajah.

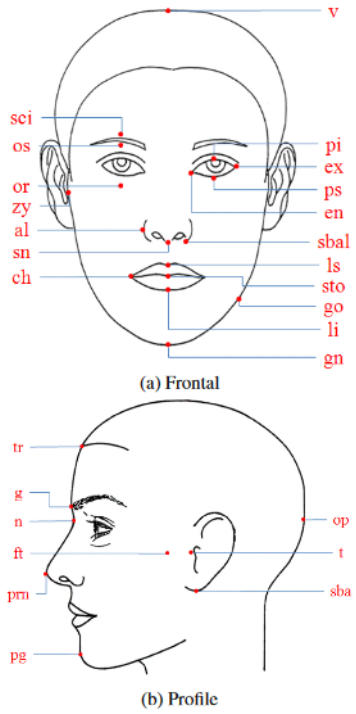
Mekanisme dasar persepsi wajah pada manusia telah dipelajari untuk dua tujuan: (a) untuk merancang sistem pengenalan mesin yang dapat meniru kemampuan manusia untuk mengenali wajah dan (b) untuk memahami mekanisme neurologis atau psikologis fungsi otak untuk perawatan medis. Karena sulit untuk mengamati secara langsung fungsi otak yang terkait dengan pengenalan wajah, pengamatan tidak langsung biasanya dilakukan untuk memahami mekanisme yang mendukung pengenalan wajah manusia. Misalnya, berdasarkan pengamatan bahwa manusia dapat mengenali karikatur dan wajah kartun, disimpulkan bahwa manusia memahami wajah berdasarkan karakteristik tingkat tinggi tertentu. Penelitian yang menggunakan teknik pencitraan otak tingkat lanjut seperti pencitraan resonansi magnetik fungsional (fMRI) diharapkan dapat mengungkap mekanisme pemrosesan wajah yang tepat di otak manusia.

Citra wajah seseorang dapat menunjukkan berbagai macam perubahan yang membuat pengenalan wajah otomatis menjadi tugas yang menantang. Misalnya, citra wajah pada (b), (c), dan (d) berbeda dari citra wajah frontal orang pada (a) dalam hal pose, iluminasi, dan ekspresi, masing-masing. Baris kedua menunjukkan variabilitas yang diperkenalkan karena penuaan. Di sini, citra pada (e), (f), dan (g) diperoleh saat orang pada (a) masing-masing berusia 32, 21, dan 15 tahun lebih muda. Baris ketiga menggambarkan masalah oklusi beberapa fitur wajah karena orang tersebut mengenakan aksesori seperti (h) kacamata resep, (i) kacamata hitam, (j) topi, dan (k) syal.

Ciri-ciri wajah

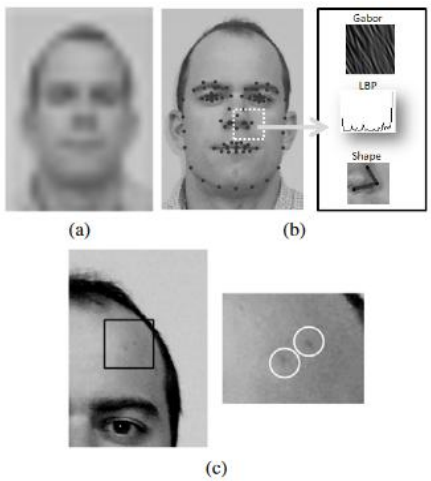
Seperti yang ditunjukkan sebelumnya, wajah terdiri dari dahi, alis, mata, hidung, mulut, pipi, dan dagu. Studi antropometri telah berupaya mengkarakterisasi dimensi wajah berdasarkan serangkaian titik acuan atau titik fiducial yang bermakna secara anatomis. Gambar 3.4 menunjukkan titik acuan representatif yang digunakan dalam beberapa studi antropometri. Pengukuran antropometri telah digunakan untuk mempelajari pola pertumbuhan pada manusia serta memahami karakteristik wajah yang berkaitan dengan jenis kelamin dan etnis. Komunitas forensik telah menggunakan titik acuan ini untuk

mengidentifikasi citra wajah. Namun, pengukuran ini tidak banyak digunakan dalam sistem pengenalan wajah otomatis karena dianggap kurang khas. Selain itu, mengekstraksi titik acuan ini dalam citra wajah berkualitas buruk mungkin sulit.



Gambar 3.4 Landmark antropometri wajah pada pandangan (a) frontal dan (b) profil wajah (Diadaptasi dari Antropometri Kepala dan Wajah, 1994).

Mirip dengan kasus sidik jari, karakteristik wajah dapat diatur ke dalam tiga tingkat berikut: (lihat Gambar 3.5).



Gambar 3.5 Contoh tiga tingkatan fitur wajah.

(a) Fitur tingkat 1 berisi informasi penampilan yang dapat berguna untuk menentukan etnis, jenis kelamin, dan bentuk umum wajah. (b) Fitur tingkat 2 memerlukan pemrosesan terperinci untuk pengenalan wajah. Informasi mengenai struktur dan bentuk serta tekstur spesifik daerah lokal di wajah digunakan untuk membuat penentuan identitas subjek yang akurat. (c) Fitur tingkat 3 meliputi tanda, tahi lalat, bekas luka, dan fitur mikro

wajah tidak teratur lainnya. Informasi ini berguna untuk mengatasi ambiguitas saat membedakan saudara kembar identik, atau untuk membantu dalam skenario investigasi forensik.

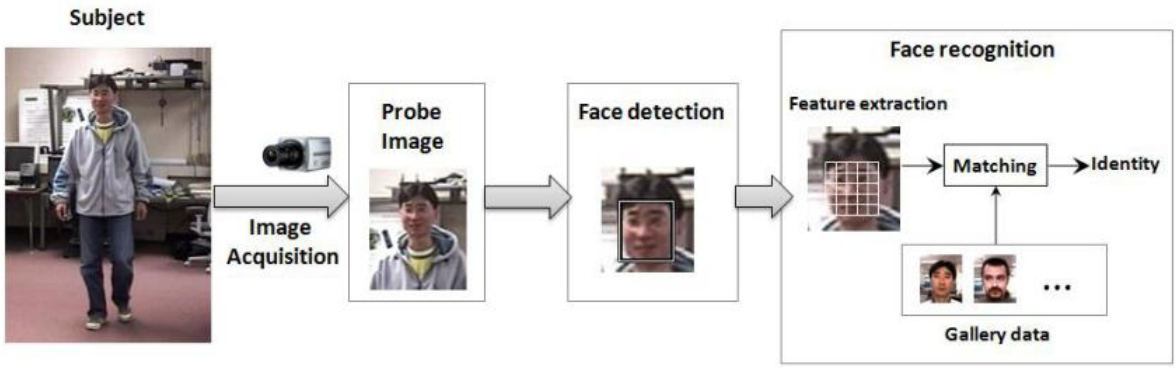
Rincian tingkat 1 terdiri dari karakteristik wajah kasar yang mudah diamati. Contohnya meliputi geometri umum wajah dan warna kulit global. Fitur-fitur tersebut dapat digunakan untuk membedakan dengan cepat antara (a) wajah bulat pendek dan wajah tipis memanjang; (b) wajah yang menunjukkan karakteristik dominan pria dan wanita; atau (c) wajah dari ras yang berbeda. Fitur-fitur ini dapat diekstraksi bahkan dari gambar wajah beresolusi rendah (<30 jarak interpupilary (IPD)1).

Detail level 2 terdiri dari informasi wajah lokal seperti struktur komponen wajah (misalnya, mata), hubungan antara komponen wajah, dan bentuk wajah yang tepat. Fitur-fitur ini penting untuk pengenalan wajah yang akurat, dan memerlukan gambar wajah beresolusi lebih tinggi (30 hingga 75 IPD). Karakteristik daerah lokal wajah dapat direpresentasikan menggunakan deskriptor geometris atau tekstur.

Detail level 3 terdiri dari fitur level mikro yang tidak terstruktur pada wajah, yang meliputi bekas luka, bintik-bintik, perubahan warna kulit, dan tahi lalat. Salah satu masalah pengenalan wajah yang menantang di mana detail Level 3 mungkin penting adalah diskriminasi saudara kembar identik.

Desain sistem pengenalan wajah

Sistem pengenalan wajah pada umumnya terdiri dari tiga modul: (a) akuisisi citra, (b) deteksi wajah, dan (c) pencocokan wajah (lihat Gambar 3.6). Citra wajah yang diperoleh dari sensor dapat dikategorikan berdasarkan (a) pita spektral (misalnya, tampak, inframerah, dan termal) yang digunakan untuk merekam citra dan (b) sifat teknik pemrosesan citra (misalnya, 2D, 3D, dan video). Karena sebagian besar sistem pengenalan wajah otomatis menggunakan citra 2D yang diperoleh dalam spektrum tampak, sebagian besar bab ini akan membahas pemrosesan jenis citra ini.



Gambar 3.6 Skema proses pengenalan wajah.

Deteksi wajah (juga dikenal sebagai pelokalan atau segmentasi wajah) mengacu pada proses penentuan lokasi wajah dalam citra dan penentuan luas spasialnya. Tugas ini dapat menjadi tantangan yang signifikan ketika objek wajah berada di latar belakang yang berantakan atau ketika beberapa citra wajah pada skala yang berbeda tersedia dalam citra

yang sama. Karena pola karakteristik mata yang khas, sebagian besar mesin pengenalan wajah komersial pertama-tama mendeteksi kedua mata sebelum menentukan lokasi spasial wajah. Deteksi wajah dalam gambar 3D dianggap sebagai masalah yang lebih mudah dibandingkan dengan gambar 2D karena tersedianya informasi kedalaman. Dalam aliran video, deteksi wajah dapat dibuat tangguh dengan melacak wajah yang terdeteksi pada serangkaian gambar. Pencocokan wajah biasanya dilakukan dengan membandingkan fitur yang diekstraksi dari probe dan gambar galeri.

3.2 AKUISISI GAMBAR

Pengenalan wajah otomatis mengharuskan data wajah berada dalam format yang dapat dibaca mesin. Foto 2D konvensional, gambar rentang atau kedalaman 3D, dan video adalah tiga jenis format gambar utama yang digunakan dalam sistem pengenalan wajah. Teknologi penginderaan terus ditingkatkan untuk meningkatkan resolusi gambar, menangkap lebih banyak detail dengan merekam wajah menggunakan beberapa spektrum (yaitu, tampak, inframerah, dan inframerah dekat), dan memfasilitasi pengoperasian sensor 3D secara real-time.

Gambar 3.7 memperlihatkan beberapa kamera 2D yang digunakan saat ini.

Sensor 2D

Sebelum perangkat canggih untuk menangkap informasi wajah dalam spektrum 3D dan tak kasat mata dikembangkan, citra fotografi dua dimensi (juga dikenal sebagai foto tersangka atau gambar diam) merupakan satu-satunya sumber yang digunakan oleh sistem pengenalan wajah otomatis. Oleh karena itu, sejumlah besar sensor dan teknik pengenalan wajah telah dikembangkan untuk memperoleh dan memproses citra wajah 2D yang berkaitan dengan spektrum kasat mata.

Karena wajah adalah objek 3 dimensi, gambar 2D wajah dapat menutupi beberapa fitur wajah. Fenomena ini disebut sebagai self-occlusion. Secara umum, tampilan depan wajah mengandung lebih banyak detail daripada tampilan profil dan karenanya, tampilan depan wajah yang cocok diharapkan dapat memberikan pengenalan orang yang lebih akurat. Konfigurasi multikamera yang menangkap gambar wajah pada beberapa sudut pose telah digunakan untuk mengatasi masalah variasi pose. Sistem pengenalan berdasarkan gambar

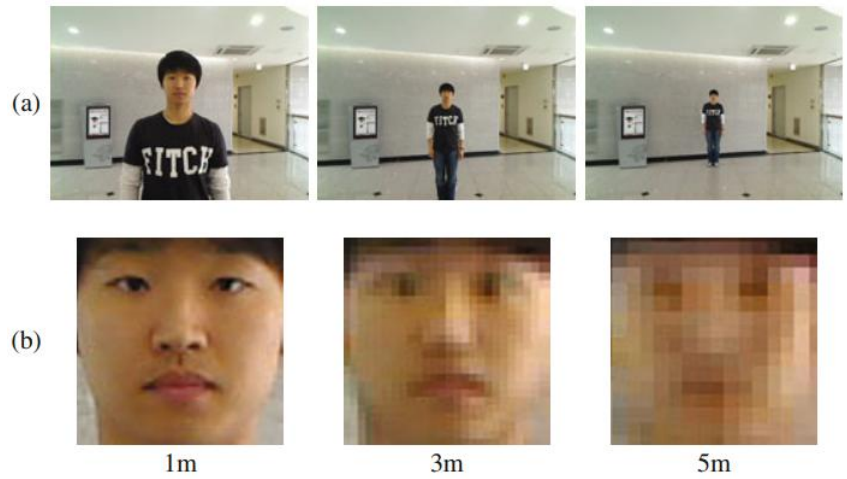
wajah 2D juga sangat dipengaruhi oleh variasi pencahayaan dan resolusi spasial. Untuk mengatasi tantangan ini, sensor baru seperti kamera resolusi tinggi, kamera pan-tilt-zoom (PTZ) aktif, dan kamera inframerah sedang digunakan.

Gambar 3.8 menunjukkan contoh gambar yang diambil dalam pita spektral tampak dan inframerah dekat (NIR). Kamera NIR dapat beroperasi bahkan dalam kondisi pencahayaan rendah karena menggunakan iluminator NIR terpisah. Karena pencahayaan NIR tidak terlihat oleh mata manusia, kamera seperti itu dapat digunakan untuk akuisisi wajah rahasia di lingkungan yang gelap (misalnya, malam).

Gambar 3.8 Gambar wajah yang ditangkap dalam spektrum tampak dan inframerah dekat pada panjang gelombang yang berbeda.

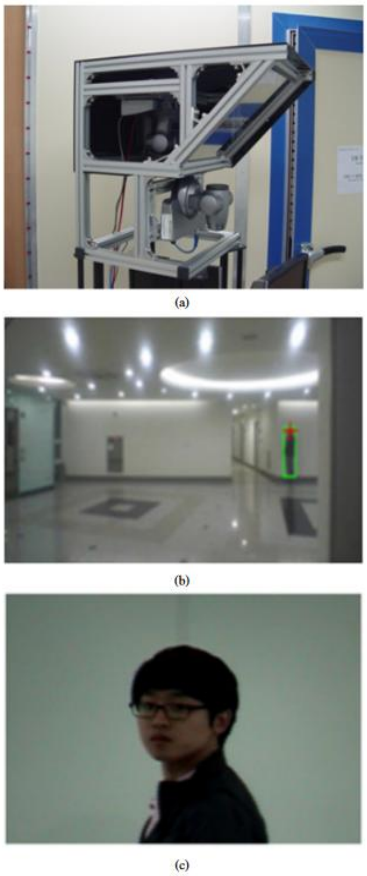
Sistem akuisisi wajah yang umum memiliki jarak operasi pendek yang terbatas pada sekitar 1-2 meter. Ketika subjek diamati pada jarak yang lebih jauh, wajah ditangkap pada resolusi rendah (lihat Gambar 3.9), yang dapat menyebabkan proses pengenalan wajah gagal. Salah satu pendekatan untuk menangani masalah resolusi spasial rendah adalah dengan menghasilkan gambar wajah beresolusi lebih tinggi dari gambar beresolusi rendah yang diberikan melalui proses yang disebut resolusi super.

Pendekatan lain untuk meningkatkan resolusi gambar wajah adalah dengan menggunakan kamera resolusi tinggi atau kamera PTZ. Kamera PTZ dapat memperbesar atau memperkecil secara dinamis untuk mendapatkan gambar close-up dari objek yang diinginkan. Namun, bidang pandang kamera PTZ sangat berkurang saat memperbesar objek. Oleh karena itu, sistem kamera dengan kamera statis dan PTZ yang dipasangkan telah muncul sebagai metode yang menjanjikan untuk mencapai kemampuan pembesaran di area pengawasan yang luas. Kamera statis menyediakan bidang pandang yang lebar dan kemudian mengarahkan kamera PTZ untuk mendapatkan gambar resolusi tinggi dari objek target. Gambar 3.10 menunjukkan contoh sistem akuisisi wajah dengan sepasang kamera statis dan PTZ serta gambar yang diambil masing-masing dari kamera statis dan PTZ.



Gambar 3.9 Gambar yang direkam oleh kamera 2D biasa dengan resolusi 640 480 saat pengguna berada pada tiga jarak berbeda dari kamera (berkisar dari 1m hingga 5m).

Baris pertama (lihat (a)) menunjukkan gambar yang diambil oleh kamera, sedangkan baris kedua (lihat (b)) menunjukkan gambar wajah yang diambil setelah pendeteksian dan pengubahan ukuran wajah. Jarak antarpupil (IPD) adalah 35, 12, dan 7 piksel untuk gambar wajah yang diambil pada jarak 1m, 3m, dan 5m. Contoh ini menggambarkan penurunan tajam dalam resolusi spasial gambar wajah saat pengguna berada jauh dari kamera.



Gambar 3.10 Contoh pengambilan gambar wajah saat subjek berada jauh dari kamera.

(a) Sistem kamera yang terdiri dari kamera statis dan kamera Pan-Tilt-Zoom (PTZ), (b) gambar orang yang diambil menggunakan kamera statis saat orang tersebut berjalan memasuki ruangan dari kanan, dan (c) gambar close-up orang yang diambil menggunakan kamera PTZ.

Sensor 3D

Masalah pose, ekspresi, dan variasi pencahayaan yang melekat pada gambar wajah 2D berasal dari rendering 2D objek wajah 3D. Upaya untuk memperoleh biometrik wajah dalam format 3D telah menghasilkan pengembangan sistem penangkapan wajah 3D. Ada dua jenis sistem penangkapan wajah 3D: satu didasarkan pada pemindaian laser dan yang lainnya didasarkan pada rekonstruksi stereografik. Secara umum dianggap bahwa pemindai laser memberikan model wajah 3D yang lebih akurat, sementara kamera stereografik memberikan kemampuan penangkapan hampir secara real-time dengan sedikit kehilangan akurasi. Gambar 3.11 menunjukkan beberapa sensor 3D yang digunakan saat ini.

Gambar 3.11 Contoh kamera 3D.

(a) Pemindai Laser 3D Konica Minolta (VIVID 9i). (b) Pemindai 3D Cyberware Rapid. (c) Pembaca Wajah 3D FastPassTM dari solusi Identitas L-1.

Gambar yang ditangkap oleh sensor 3D biasanya mencakup sekitar 120^{o} kepala manusia dan gambar ini disebut sebagai pemindaian 2.5D. Jika diperlukan model 3D wajah yang lengkap, model tersebut dapat dibuat dengan menggabungkan sekitar tiga hingga lima pemindaian 2.5D yang diambil dari beberapa tampilan. Model wajah 3D biasanya direpresentasikan sebagai struktur jaring poligonal (misalnya, segitiga atau persegi panjang) untuk efisiensi komputasi (lihat Gambar 3.12). Struktur jaring 3D berubah tergantung pada praproses (misalnya, penghalusan, pengisian lubang, dll.), konstruksi jaring, dan proses pencitraan (pemindaian dengan sensor laser).

(a) (b)

Gambar 3.12 (a) Model 3D penuh wajah manusia yang diperoleh menggunakan sensor 3D. (b) Model wajah 3D yang direpresentasikan menggunakan jaring segitiga.

Meskipun geometri 3D model wajah berubah tergantung pada pose, perubahan ini sangat kecil dan model tersebut secara umum dianggap tidak berubah terhadap pose. Lebih jauh, model tersebut juga kuat terhadap variasi pencahayaan. Akan tetapi, pengenalan wajah 3D tidak invarian terhadap perubahan ekspresi, penuaan, dan oklusi. Kelemahan akuisisi wajah 3D meliputi waktu akuisisi gambar yang lebih lama, ukuran data model 3D yang besar (yang memerlukan sumber daya komputasi yang lebih tinggi selama pencocokan), dan harga sensor pencitraan 3D yang relatif tinggi.

Rangkaian video

Kamera video dapat terus-menerus menangkap gambar wajah, sehingga memungkinkan pemilihan gambar wajah berkualitas baik (misalnya, gambar dengan pose frontal dan ekspresi netral) untuk pengenalan. Penurunan harga kamera video juga menjadikannya solusi yang lebih layak untuk sistem pengenalan wajah. Sensor berbasis video biasanya menyediakan gambar beresolusi lebih rendah dibandingkan dengan sensor 2D diam untuk menangani sejumlah besar data yang mengalir dari sensor ke unit penyimpanan atau pemrosesan (30 bingkai per detik dalam standar Komite Sistem Televisi Nasional). Teknik kompresi video juga biasanya digunakan untuk menangani aliran data besar, yang dapat memengaruhi kualitas gambar yang diperoleh dalam mode ini.

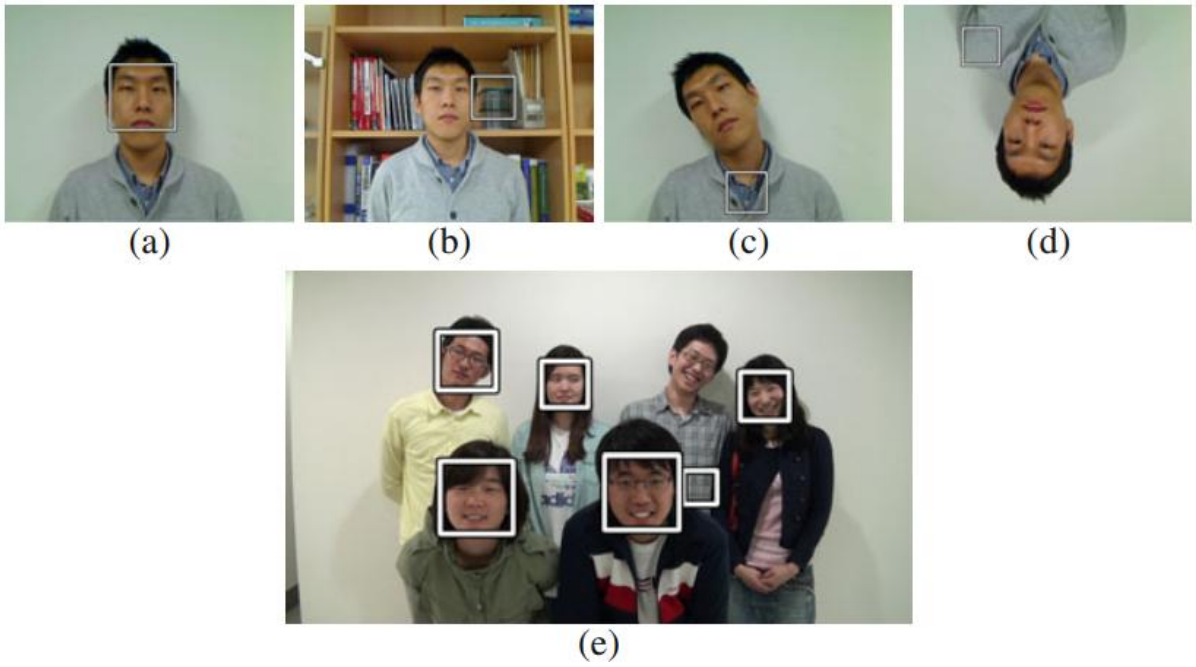
Ada minat yang signifikan dalam mengembangkan sistem pengenalan wajah yang kuat yang akan menerima aliran video sebagai masukan. Pengenalan wajah dalam video telah menarik minat karena penyebaran kamera pengintai yang meluas. Kemampuan untuk mengenali wajah secara otomatis secara real-time dari video akan memfasilitasi, antara lain, metode rahasia untuk identifikasi manusia menggunakan jaringan kamera pengintai yang ada. Dua informasi khas disediakan oleh aliran video: (a) beberapa bingkai dari subjek yang sama dan (b) informasi temporal yang berkaitan dengan wajah seseorang. Beberapa bingkai biasanya menggambarkan berbagai pose, memungkinkan pemilihan bingkai berkualitas baik yang tepat (yaitu, gambar wajah berkualitas tinggi dalam pose hampir frontal) untuk kinerja pengenalan yang unggul. Informasi temporal dalam video sesuai dengan gerakan wajah dinamis dalam video. Namun, sulit untuk menentukan apakah ada detail terkait identitas dalam gerakan wajah (penelitian dalam psikologi telah menunjukkan bahwa gerakan wajah memiliki beberapa informasi diskriminatif yang mungkin berguna dalam menetapkan identitas).

3.3 DETEKSI WAJAH

Deteksi wajah merupakan langkah pertama dalam sebagian besar aplikasi yang berhubungan dengan wajah, termasuk pengenalan wajah, analisis ekspresi wajah, klasifikasi jenis kelamin/etnis/usia, dan pemodelan wajah. Variasi dalam pose dan ekspresi, keragaman jenis kelamin dan warna kulit, serta oklusi (misalnya, karena kacamata) merupakan tantangan umum yang membingungkan dalam deteksi wajah.

Meskipun ada sejumlah pendekatan untuk mendeteksi wajah dalam gambar tertentu, metode deteksi wajah terkini biasanya didasarkan pada ekstraksi fitur tekstur lokal dari gambar yang diberikan dan penerapan pengklasifikasi biner (dua kelas) untuk membedakan antara wajah dan bukan wajah. Pendekatan ini mengikuti karya penting yang dilakukan oleh Viola dan Jones dalam bidang deteksi objek waktu nyata.

Teknik deteksi wajah yang diusulkan oleh Viola dan Jones telah banyak digunakan dalam berbagai penelitian yang melibatkan pemrosesan wajah karena kemampuannya secara real-time, akurasinya yang tinggi, dan ketersediaannya sebagai perangkat lunak sumber terbuka di bawah Open Computer Vision Library (OpenCV). Akan tetapi, detektor wajah Viola-Jones tidaklah sempurna dan dapat menghasilkan kesalahan positif palsu dan kesalahan negatif palsu seperti yang ditunjukkan pada Gambar 3.13. Kesalahan positif palsu mengacu pada deteksi wajah padahal sebenarnya tidak ada, sedangkan kesalahan negatif palsu menunjukkan bahwa wajah yang ada dalam gambar tidak terdeteksi.



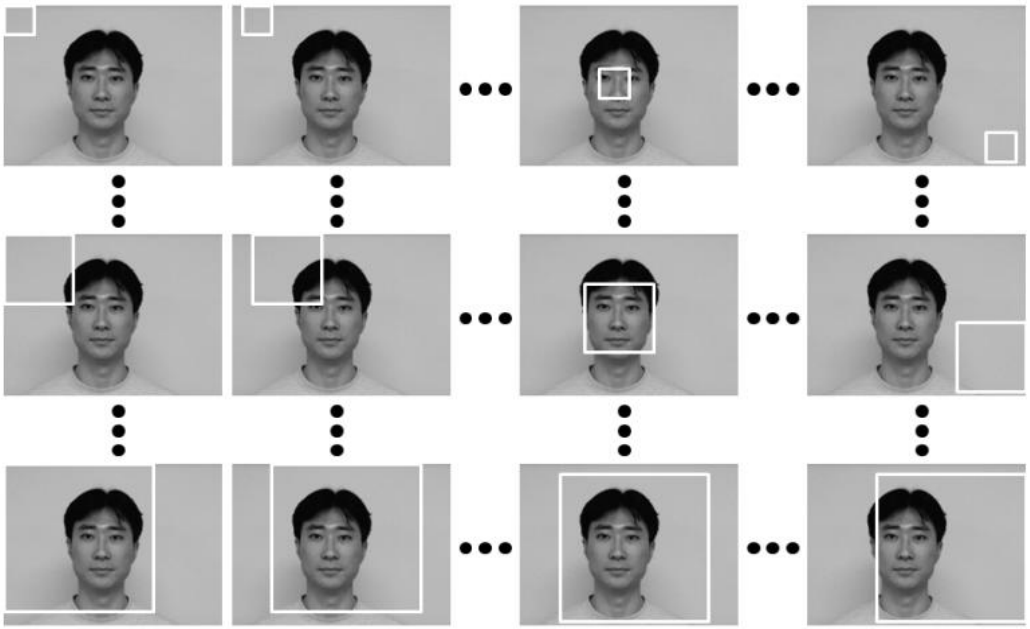
Gambar 3.13 Masalah deteksi wajah melibatkan pendeteksian wajah dalam gambar.

Algoritma deteksi wajah harus tangguh terhadap variasi pencahayaan, latar belakang, rotasi, dan resolusi gambar. Dalam gambar ini, output algoritma deteksi wajah Viola-Jones, sebagaimana diterapkan dalam Open Computer Vision Library (OpenCV), ditampilkan untuk berbagai skenario: (a) latar belakang sederhana, (b) latar belakang berantakan, (c) wajah miring, (d) wajah terbalik, dan (e) beberapa wajah. Gambar (b) hingga (e) memiliki negatif palsu (wajah yang tidak terdeteksi) dan positif palsu (daerah non-wajah salah dikategorikan sebagai wajah).

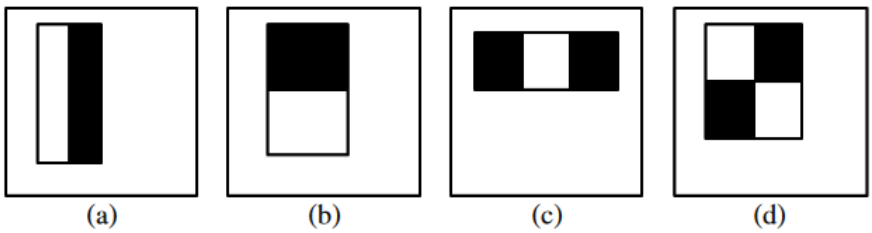
Detektor wajah Viola-Jones

Detektor wajah Viola-Jones memindai gambar masukan dengan jendela deteksi dengan ukuran berbeda dan memutuskan apakah setiap jendela berisi wajah atau tidak. Gambar 3.14 menunjukkan proses pemindaian mulai dari jendela kecil hingga besar. Di setiap jendela, keberadaan kandidat wajah diputuskan dengan menerapkan pengklasifikasi

ke fitur lokal sederhana yang diturunkan menggunakan filter persegi panjang. Filter persegi panjang ini dapat dikelompokkan sebagai filter dua persegi panjang, tiga persegi panjang, dan empat persegi panjang seperti yang ditunjukkan pada Gambar 3.15. Karena filter persegi panjang 2D ini mirip dengan wavelet Haar satu dimensi yang digunakan dalam domain pemrosesan sinyal, filter ini juga dikenal sebagai filter mirip Haar. Nilai fitur diperoleh dengan menghitung perbedaan antara jumlah intensitas piksel di daerah persegi panjang terang dan gelap. Misalnya, filter tiga persegi panjang dapat digunakan untuk mendeteksi dua mata dan pangkal hidung. Ini karena mata biasanya memiliki nilai intensitas yang lebih gelap dibandingkan dengan pangkal hidung dan penerapan filter tiga persegi panjang berfungsi untuk lebih memperkuat perbedaan ini. Penggunaan fitur tingkat rendah tersebut, alih-alih nilai piksel mentah, memungkinkan deteksi wajah lebih cepat serta memberikan ketahanan terhadap perubahan pencahayaan dan perspektif.



Gambar 3.14 Metode Viola-Jones menggunakan jendela dengan ukuran berbeda untuk "memindai" seluruh gambar guna menentukan lokasi wajah. Dalam contoh di atas, jendela di kolom ketiga baris kedua kemungkinan akan terdeteksi sebagai wajah.



Gambar 3.15 Metode Viola-Jones menggunakan berbagai jenis filter mirip Haar untuk deteksi wajah.

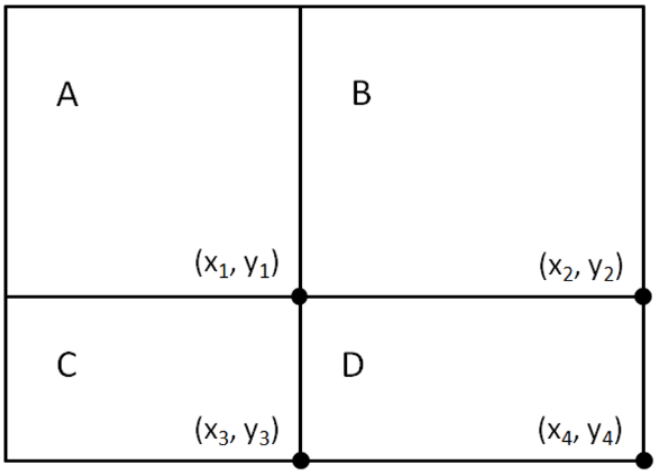
Filter ini diterapkan pada setiap jendela yang memindai citra masukan. Ketika kombinasi respons filter (fitur) pada jendela tertentu melampaui ambang batas, wajah dikatakan telah terdeteksi. Di sini, (a) dan (b) adalah

filter dua persegi panjang, (c) adalah filter tiga persegi panjang, dan (d) adalah filter empat persegi panjang. Perhatikan bahwa filter ditampilkan relatif terhadap jendela deteksi (persegi panjang luar).

Tidak ada satu pun filter mirip Haar yang dapat melakukan tugas deteksi wajah dengan akurasi tinggi. Oleh karena itu, serangkaian filter mirip Haar dengan ukuran berbeda perlu diterapkan ke setiap jendela dan respons filter harus digabungkan dengan cara yang tepat guna mendeteksi wajah. Akibatnya, jumlah fitur di setiap jendela deteksi bisa sangat besar. Misalnya, lebih dari 180.000 fitur mirip Haar yang berbeda dapat diperoleh dari jendela deteksi berukuran 24 x 24 piksel. Beban komputasi yang terlibat dalam komputasi fitur-fitur ini dapat dikurangi secara signifikan dengan melakukan pra-komputasi gambar integral dari gambar asli. Citra integral S yang terkait dengan citra I yang diberikan dapat dihitung sebagai berikut:

$$S(x,y) = \sum_{1 \le x' \le x, 1 \le y' \le y} I(x',y') \tag{3.1}$$

di mana $I(x,y)$ adalah nilai intensitas piksel (x,y) pada gambar asli dan $S(x,y)$ adalah nilai piksel terkait pada gambar integral. Dengan demikian, gambar integral pada lokasi (x,y) berisi jumlah semua intensitas piksel di atas dan di sebelah kiri (x,y) pada gambar asli. Gambar integral dapat dihitung dengan cepat dalam satu lintasan pada gambar asli. Setelah gambar integral tersedia, jumlah nilai piksel dalam setiap wilayah persegi panjang sembarang pada gambar asli dapat dihitung berdasarkan hanya empat akses array seperti yang ditunjukkan pada Gambar 3.16.



Gambar 3.16 Penggunaan citra integral mempercepat komputasi fitur dalam detektor wajah Viola-Jones.

Misalkan nilai citra integral pada titik (x_1, y_1), (x_2, y_2), (x_3, y_3), dan (x_4, y_4) masing-masing adalah S(x_1, y_1), S(x_2, y_2), S(x_3, y_3), dan S(x_4, y_4). Dengan demikian, jumlah nilai piksel dalam persegi panjang D dapat dihitung sebagai S(x_4, y_4) − S(x_2, y_2) − S(x3, y_3)+ S(x_1, y_1).

Meskipun gambar integral memungkinkan perhitungan nilai fitur yang efisien, hal itu tidak mengurangi kompleksitas komputasi ke tingkat yang cukup untuk deteksi wajah secara

real-time. Untuk mencapai deteksi real-time, penting untuk menentukan sebagian kecil fitur diskriminatif dari set lengkap fitur yang tersedia dalam setiap jendela. Dengan mengevaluasi hanya subset fitur yang lebih kecil ini dan menggabungkannya menggunakan fungsi yang sesuai, detektor wajah yang cepat dan efektif dapat diperoleh. Varian algoritma Adaboost yang diusulkan dalam literatur pengenalan pola dapat digunakan untuk memilih fitur diskriminatif serta untuk melatih fungsi pengklasifikasi.

Fungsi pengklasifikasi menggabungkan nilai fitur menggunakan bobot yang sesuai dan jika nilai gabungan lebih besar dari ambang batas, jendela tersebut diklasifikasikan sebagai citra wajah.

Algoritma pemilihan fitur dan pelatihan pengklasifikasi bekerja sebagai berikut. Misalkan $f_j(w)$ adalah nilai fitur yang diperoleh dengan menerapkan filter f_j ke jendela deteksi $w, j = 1, 2, \dots, L$, di mana L adalah jumlah total filter. Jendela deteksi w diparameterisasi berdasarkan lokasi dan ukurannya. Setiap nilai fitur dapat digunakan untuk membangun pengklasifikasi lemah yang memprediksi apakah jendela w adalah citra wajah. Pengklasifikasi lemah tersebut dapat didefinisikan sebagai

$$h_j(w) \begin{cases} 1 \text{ jika } p_j f_j(w) \leq p_j \theta_j \\ 0 \text{ Lainnya} \end{cases} \tag{3.2}$$

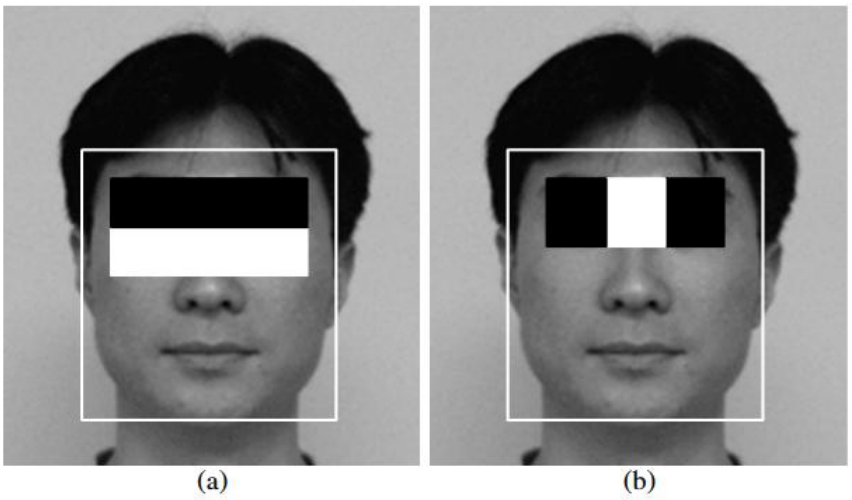
di mana p_j adalah tanda (+ atau -) yang menentukan arah pertidaksamaan, θ_j adalah ambang batas, dan $j = 1, 2, \dots, L$. Diberikan satu set pelatihan dari n contoh gambar yang mencakup wajah dan bukan wajah, pengklasifikasi dapat dilatih seperti yang dijelaskan dalam Algoritma 3. Algoritma ini memilih T fitur yang paling diskriminatif di antara L fitur dan mempelajari pengklasifikasi linier berdasarkan fitur-fitur ini. Biasanya, nilai T dipilih agar jauh lebih kecil (katakanlah dalam urutan beberapa ratus) daripada nilai L. Proses pelatihan di atas dapat dilakukan secara luring. Selama tahap deteksi wajah yang sebenarnya, hanya nilai fitur T yang perlu dihitung untuk setiap jendela dan keluaran dari pengklasifikasi lemah berdasarkan fitur-fitur ini perlu digabungkan menggunakan fungsi linier. Ini memungkinkan kategorisasi cepat setiap jendela menjadi wajah atau bukan wajah.

Namun, gambar asli masih harus dipindai dengan jendela dengan ukuran berbeda untuk menentukan lokasi wajah. Gambar 3.17 menunjukkan dua fitur mirip Haar yang paling efektif yang mampu menolak sekitar 60% non-wajah. Fitur pertama menunjukkan fakta bahwa daerah mata biasanya lebih gelap daripada daerah pipi. Fitur kedua menyoroti pangkal hidung yang lebih terang dibandingkan dengan daerah mata. Pengklasifikasi dengan satu set filter yang lebih kecil dan sederhana dapat digunakan pertama kali untuk menyaring sejumlah besar gambar non-wajah pada tahap awal dan kemudian pengklasifikasi yang lebih kuat dapat digunakan pada tahap selanjutnya. Skema pengklasifikasi kaskade tersebut ditunjukkan pada Gambar 3.18.

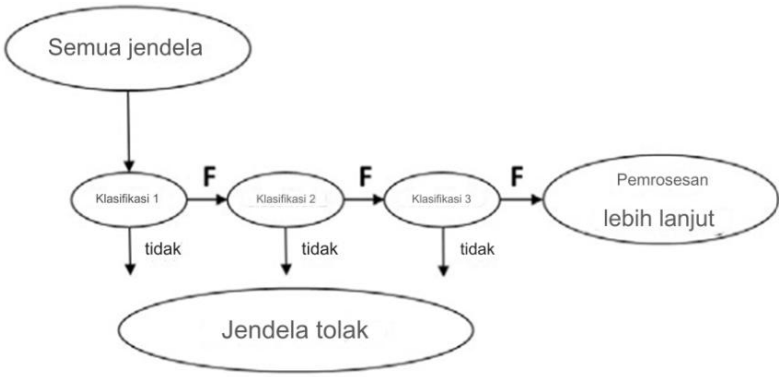
Karena teknik deteksi wajah Viola-Jones merupakan pendekatan deteksi objek generik, teknik yang sama dapat digunakan untuk mendeteksi komponen individual dalam citra wajah yang terdeteksi. Misalnya, detektor mata dapat dibangun hanya dengan

mengganti set pelatihan dengan contoh citra mata dan citra non-mata. Gambar 3.19 menunjukkan contoh hasil deteksi wajah dan mata menggunakan detektor wajah Viola-Jones di OpenCV.

Meskipun detektor wajah Viola-Jones telah menunjukkan kinerja yang sangat baik dalam aplikasi waktu nyata, detektor ini masih kesulitan saat berhadapan dengan pose wajah non-frontal, perubahan pencahayaan, oklusi, dll. Ada sejumlah pendekatan serupa yang diusulkan untuk deteksi wajah yang lebih efektif dan efisien. Skema ini menggunakan fitur yang lebih tangguh termasuk fitur mirip Haar dengan variasi rotasi, tepi, isyarat gerakan, dan Pola Biner Lokal (LBP) atau menggunakan algoritme pembelajaran yang lebih baik dibandingkan dengan implementasi Adaboost.

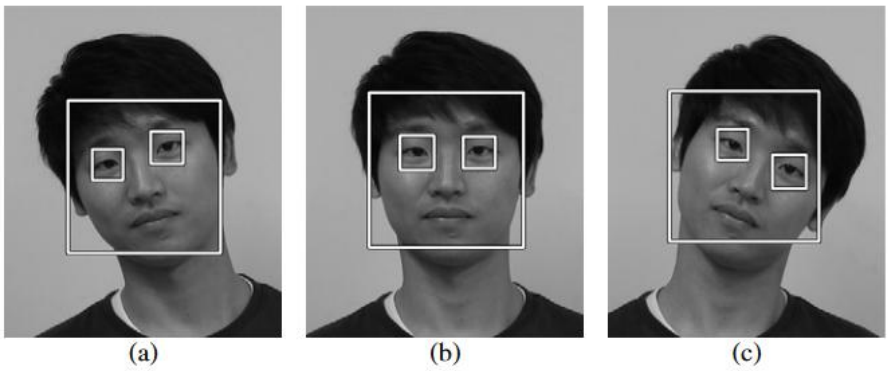


Gambar 3.17 Dua fitur mirip Haar yang paling diskriminatif dihamparkan pada gambar masukan.



Gambar 3.18 Skema pengklasifikasi bertingkat untuk mempercepat proses deteksi wajah.

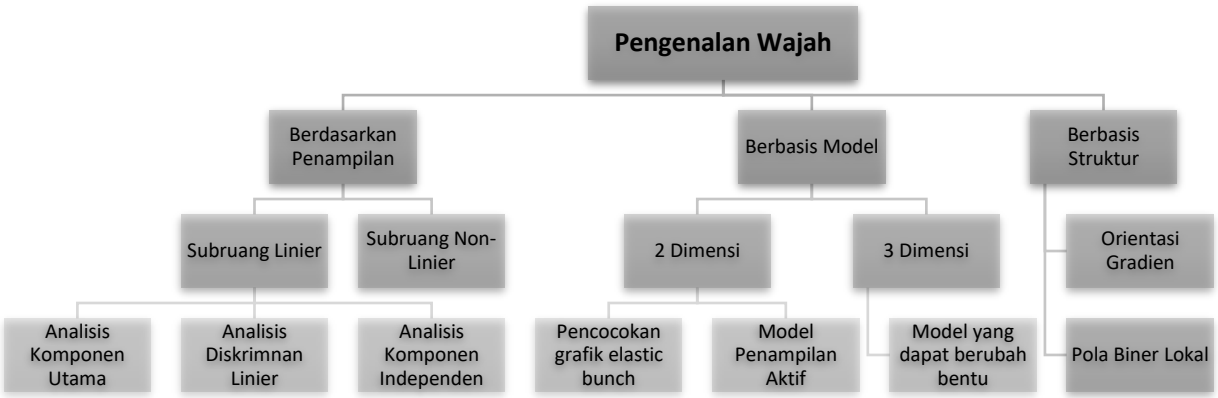
Pengklasifikasi awal hanya menggunakan beberapa fitur dan menghilangkan sejumlah besar non-wajah dengan pemrosesan minimal. Pengklasifikasi berikutnya mempertimbangkan lebih banyak fitur dan selanjutnya menghilangkan non-wajah yang tersisa dengan biaya pemrosesan tambahan. Di sini, F menunjukkan bahwa pengklasifikasi memutuskan bahwa jendela yang diuji berisi kandidat wajah, sementara NF mewakili keputusan pengklasifikasi bahwa tidak ada kandidat wajah dalam jendela yang diuji.



Gambar 3.19 Contoh deteksi wajah dan mata menggunakan pendekatan deteksi objek Viola-Jones.

3.4 EKSTRAKSI DAN PENCOCOKAN FITUR

Ada tiga pendekatan utama untuk mencocokkan gambar wajah yang terdeteksi (lihat Gambar 3.20): metode berbasis tampilan, berbasis model, dan berbasis tekstur. Teknik berbasis tampilan menghasilkan representasi kompak dari seluruh wilayah wajah dalam gambar yang diperoleh dengan memetakan gambar wajah berdimensi tinggi ke dalam subruang berdimensi lebih rendah.



Gambar 3.20 Kategorisasi teknik pengenalan wajah.

Subruang ini didefinisikan oleh sekumpulan vektor basis representatif, yang dipelajari menggunakan sekumpulan gambar pelatihan. Meskipun pemetaan dapat berupa linear atau non-linear, skema yang umum digunakan seperti Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), dan Independent Component Analysis (ICA) melibatkan proyeksi linear.

Teknik berbasis model mencoba membangun model wajah 2D atau 3D yang memfasilitasi pencocokan gambar wajah dengan adanya variasi pose. Sementara *Face Bunch Graphs* (FBG) dan *Active Appearance Model* (AAM) adalah contoh model wajah 2D, model yang dapat diubah adalah model 3D. Pendekatan berbasis tekstur mencoba menemukan fitur lokal yang kuat yang tidak berubah terhadap variasi pose atau pencahayaan. Contoh fitur tersebut termasuk orientasi gradien dan *Local Binary Patterns* (LBP).

Baru-baru ini, skema yang memanfaatkan model 3D, input video, dan detail tingkat mikro (misalnya, bintik-bintik, tahi lalat, bekas luka) telah dikembangkan untuk meningkatkan akurasi sistem pengenalan wajah. Meskipun bagian ini menjelaskan beberapa skema representatif untuk mencocokkan gambar diam 2D, beberapa perkembangan terkini dibahas di Bagian 3.5.

Pengenalan wajah berbasis penampilan

Skema berbasis penampilan didasarkan pada gagasan untuk merepresentasikan citra wajah yang diberikan sebagai fungsi dari berbagai citra wajah yang tersedia dalam set pelatihan, atau sebagai fungsi dari beberapa wajah dasar. Misalnya, nilai piksel pada lokasi (x, y) dalam citra wajah dapat dinyatakan sebagai jumlah tertimbang dari nilai piksel di semua citra pelatihan pada (x, y). Set citra pelatihan atau wajah dasar membentuk subruang dan jika citra wajah yang diberikan diproyeksikan secara linier ke subruang ini, maka disebut sebagai analisis subruang linier. Tantangan di sini adalah menemukan subruang berdimensi rendah yang sesuai yang mempertahankan informasi diskriminatif yang terkandung dalam citra wajah. Dengan kata lain, tujuan dalam analisis subruang linier adalah menemukan satu set kecil wajah dasar yang paling representatif. Setiap citra wajah baru dapat direpresentasikan sebagai jumlah tertimbang dari wajah dasar dan dua citra wajah dapat dicocokkan dengan membandingkan vektor bobotnya secara langsung.

Analisis Komponen Utama

Analisis Komponen Utama (PCA) adalah salah satu metode otomatis paling awal yang diusulkan untuk pengenalan wajah. PCA menggunakan data pelatihan untuk mempelajari subruang yang memperhitungkan sebanyak mungkin variabilitas dalam data pelatihan. Hal ini dicapai dengan melakukan dekomposisi nilai Eigen dari matriks kovariansi data. Secara khusus, PCA melibatkan lima langkah berikut.

1. Misalkan $\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_N}$ adalah set pelatihan, di mana setiap x_i mewakili vektor kolom berdimensi d. Hitung rata-rata set pelatihan sebagai

$$\boldsymbol{\mu} = \frac{1}{N}\sum_{i=1}^{N} \mathbf{x}_i \tag{3.3}$$

2. Tentukan matriks data $\mathbf{X}$ sebagai berikut: $\mathbf{X} = [(\mathbf{x_1} - \boldsymbol{\mu})(\mathbf{x_2} - \boldsymbol{\mu})(\mathbf{x_3} - \boldsymbol{\mu})]$.
3. Hitung matriks kovariansi data sebagai berikut:

$$\mathbf{C} = \mathbf{X}\mathbf{X}^{\mathbf{T}} \tag{3.4}$$

   di mana $\mathbf{X}^{\mathbf{T}}$ adalah transpos matriks $\mathbf{X}$. Karena $\mathbf{X}$ adalah matriks berdimensi $d \times N$, ukuran matriks kovariansi $\mathbf{C}$ adalah $d \times d$
4. Hitung vektor Eigen dari matriks kovariansi $\mathbf{C}$ dengan menyelesaikan sistem Eigen berikut.

$$\mathbf{C}\mathbf{E} = \boldsymbol{\lambda}\mathbf{E} \tag{3.5}$$

   Di sini, $\mathbf{E} = [\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_d}]$ di mana $\mathbf{e_1}, \mathbf{e_2}, \ldots, \mathbf{e_d}$ adalah vektor Eigen d dari $\mathbf{C}$.

5. Setiap vektor data $\mathbf{x}$ dapat direpresentasikan sebagai jumlah tertimbang dari vektor Eigen dan bobot ini dapat dihitung sebagai $\boldsymbol{\omega} = \mathbf{E}^{\boldsymbol{T}}\mathbf{x}, di$ mana $\mathbf{E}^{\boldsymbol{T}}$ adalah transpos dari $\mathbf{E}$. Perhatikan bahwa $\boldsymbol{\omega} = [\omega_1, \omega_2, \dots, \omega_d]^{\boldsymbol{T}}$ adalah vektor kolom d −dimensi, di mana ω_j adalah bobot yang terkait dengan vektor Eigen $\mathbf{e}_j$ untuk $j = 1, 2, , d$. Bobot ini juga dikenal sebagai koefisien Eigen.

Gambar wajah I berukuran $d_1 \times d_2$ piksel dapat secara langsung direpresentasikan sebagai vektor d-dimensi $\mathbf{x}$ yang memuat semua intensitas piksel di I, di mana $d = d_1 d_2$. Diberikan satu set gambar wajah pelatihan $I_1, I_2, \dots, I_N$, langkah-langkah PCA di atas dapat diterapkan untuk memperoleh vektor Eigen d (juga disebut sebagai Eigenfaces). Alih-alih menggunakan nilai piksel mentah, dimungkinkan juga untuk mengekstrak beberapa fitur (misalnya, orientasi gradien) dari gambar dan melakukan PCA pada vektor fitur yang dihasilkan. Untuk melakukan pencocokan wajah, koefisien Eigen $\boldsymbol{\omega}^{\mathbf{E}}$ dan $\boldsymbol{\omega}^{\mathrm{A}}$ yang sesuai dengan gambar wajah galeri dan probe, masing-masing, dapat dihitung dan jarak Euclidean antara dua koefisien Eigen dapat dianggap sebagai ukuran ketidakmiripan antara dua gambar wajah.

Dalam uraian PCA di atas, dimensionalitas koefisien Eigen (ω) sama dengan dimensionalitas data asli $\mathbf{x}$, yaitu d. Telah ditunjukkan bahwa salah satu tujuan analisis subruang linier adalah untuk mengurangi dimensionalitas. Dalam PCA, hal ini dapat dicapai dengan mempertimbangkan subruang berdimensi lebih rendah E' , yang direntangkan hanya oleh vektor Eigen $d'(d' < d)$ dari E yang sesuai dengan nilai Eigen terbesar d'. Dengan memproyeksikan data ke subruang E' , dimensionalitas koefisien Eigen menjadi d' , yang lebih kecil dari dimensi data asli d. Vektor Eigen yang sesuai dengan nilai Eigen terbesar dalam PCA memperhitungkan variabilitas maksimum dalam data dan disebut sumbu utama. Biasanya, dimungkinkan untuk memperhitungkan sebagian besar variabilitas dalam data dengan memilih hanya beberapa vektor Eigen yang sesuai dengan nilai Eigen terbesar dalam urutan menurun. Gambar 3.21 menunjukkan Eigenfaces yang sesuai dengan tujuh nilai Eigen terbesar, yang diperoleh melalui pelatihan pada gambar wajah yang terdapat dalam basis data ORL.

Gambar 3.21 Eigenface yang sesuai dengan tujuh nilai Eigen terbesar yang diperoleh dari basis data wajah ORL.

Jika jumlah sampel pelatihan (N) lebih kecil daripada dimensionalitas data (d), hanya akan ada ($N - 1$) vektor Eigen yang bermakna dan vektor Eigen yang tersisa akan memiliki nilai Eigen terkait nol. Vektor Eigen ($N - 1$) ini dapat dihitung dengan cepat menggunakan trik berikut. Tentukan $\mathbf{C}^* = \mathbf{X}^{\mathbf{T}}\mathbf{X}$ Karena $\mathbf{C}^*$ adalah matriks $N \times N$ dan $N < d$, dekomposisi

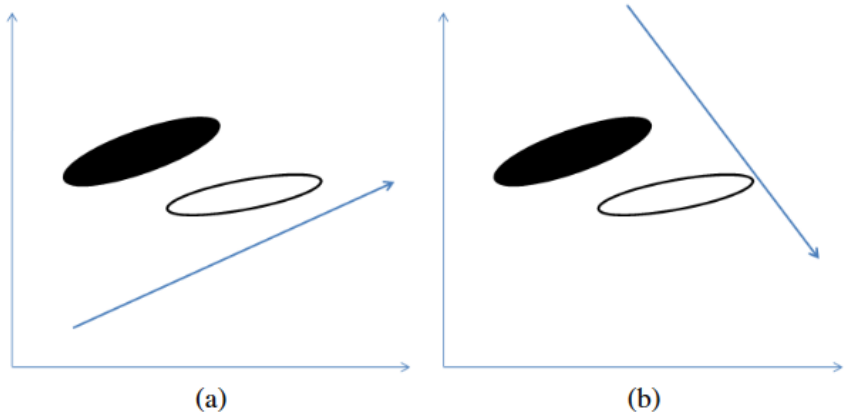
Eigen $\mathbf{C}^*$ dapat dihitung lebih efisien dibandingkan dengan $\mathbf{C}$. Biarkan $\mathbf{E}^*$ menjadi matriks yang berisi vektor Eigen $\mathbf{C}^*$. Matriks vektor Eigen yang bermakna dari $\mathbf{C}$ (yang dikaitkan dengan nilai Eigen bukan nol) dapat diperoleh sebagai $\mathbf{V} = \mathbf{X}\mathbf{E}^*$dan koefisien Eigen yang sesuai dengan vektor data x dapat dihitung sebagai $\boldsymbol{\omega} = \mathbf{V}^{\mathbf{T}}\mathbf{x}$.

Versi PCA yang lebih umum adalah Analisis Komponen Independen (ICA). PCA membatasi vektor Eigen agar ortogonal satu sama lain dan karenanya, koefisien Eigen yang dihasilkan tidak berkorelasi. Namun, koefisien Eigen tidak harus independen2. Di sisi lain, ICA mencoba menemukan transformasi linier yang meminimalkan ketergantungan statistik antara komponen-komponennya. Akibatnya, koefisien ICA bersifat independen atau "sebisa mungkin independen". Selain itu, tidak seperti PCA, tidak ada urutan relatif antara koefisien ICA. Gambar 3.22 menunjukkan tujuh komponen ICA yang diperoleh melalui pelatihan pada gambar wajah yang terdapat dalam basis data ORL.

Gambar 3.22 Tujuh komponen ICA yang berasal dari basis data wajah ORL. Perhatikan bahwa tidak ada urutan relatif antara komponen-komponen ICA.

Analisis Diskriminan Linier

PCA dapat disebut sebagai metode pembelajaran tanpa pengawasan, karena label kelas (informasi identitas pengguna) tidak pernah digunakan selama pembelajaran wajah dasar. Oleh karena itu, akurasi pengenalan wajah berdasarkan PCA tidak dapat diharapkan sangat tinggi. Analisis Diskriminan Linier (LDA) secara eksplisit menggunakan label kelas dari data pelatihan dan melakukan analisis subruang dengan tujuan meminimalkan variasi intrakelas dan memaksimalkan variasi antarkelas (lihat Gambar 3.23).



Gambar 3.23 Perbandingan PCA dan LDA untuk masalah dua kelas dengan data dua dimensi. Di sini, data yang sesuai dengan dua kelas diasumsikan ada dalam dua elips.

(a) Sumbu utama dalam PCA disejajarkan sedemikian rupa sehingga ketika data diproyeksikan ke sumbu ini, varians dimaksimalkan. (b) Sumbu utama dalam LDA disejajarkan sedemikian rupa sehingga ketika data

diproyeksikan ke sumbu ini, varians dalam setiap kelas diminimalkan dan keterpisahan antara dua kelas dimaksimalkan.

Oleh karena itu, LDA secara umum diharapkan dapat memberikan pengenalan wajah yang lebih akurat ketika sampel gambar wajah yang cukup untuk setiap pengguna tersedia selama pelatihan. Koefisien LDA dapat dihitung sebagai berikut

1. Misalkan $(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2) \ldots (\mathbf{x}_N, y_N)$ adalah himpunan pelatihan, di mana setiap $\mathbf{x}_i$ mewakili vektor kolom berdimensi $d, y_i \in \{1, 2, \ldots, c\}$ adalah label kelas yang sesuai, dan c adalah jumlah kelas. Hitunglah rata-rata setiap kelas sebagai berikut:

$$\boldsymbol{\mu}_j = \frac{1}{N_j} \sum_{y_1=j} \mathbf{x}_i \tag{3.6}$$

di mana N_j adalah jumlah sampel dari kelas j dan $j = 1, 2, , c$.

2. Tentukan matriks sebaran dalam dan antar kelas (masing-masing $\mathbf{S}_w$dan $\mathbf{S}_b$) untuk data pelatihan yang diberikan sebagai

$$\mathbf{S}_w = \sum_{j=1}^{c} \sum_{y_i=j} (x_i - \mu_j)(x_i - \mu_j)^T \tag{3.7}$$

$$\mathbf{S}_b = \sum_{j=1}^{c} N_j (\mu_j - \mu)(\mu_j - \mu)^T \tag{3.8}$$

Dimana $\mu = (1/N) \sum_{i=1}^{N} \mathbf{x}_i$

3. Subruang LDA dibangun sedemikian rupa sehingga meminimalkan $\mathbf{S}_w$ dan memaksimalkan $\mathbf{S}_b$, yang dicapai secara bersamaan dengan memaksimalkan $S_w^{-1} S_b$. Vektor Eigen yang memaksimalkan $S_w^{-1} S_b$ dapat dihitung dengan mengikuti pendekatan yang sama seperti dalam PCA, yaitu dengan menyelesaikan sistem Eigen berikut.

$$\mathbf{S_w^{-1} S_b E} = \boldsymbol{\lambda} \mathbf{E} \tag{3.9}$$

4. Setiap vektor data $\mathbf{x}$ dapat direpresentasikan sebagai jumlah tertimbang dari vektor Eigen di atas dan bobot ini dapat dihitung sebagai $\boldsymbol{\omega} = \mathbf{E}^T \mathbf{x}$, di mana $\mathbf{E}^T$ adalah transpos dari $\mathbf{E}$.

Diberikan satu set gambar wajah pelatihan $I_1, I_2, \ldots, I_N$, langkah-langkah LDA di atas dapat diterapkan untuk memperoleh vektor Eigen d dari $\mathbf{S_w^{-1} S_b}$ (juga disebut sebagai Fisherfaces). Untuk melakukan pencocokan wajah, koefisien LDA $\boldsymbol{\omega}^E$ dan $\boldsymbol{\omega}^A$ yang sesuai dengan gambar wajah galeri dan probe, masing-masing, dapat dihitung dan jarak Euclidean antara dua koefisien LDA dapat dianggap sebagai ukuran ketidaksamaan antara dua gambar wajah.

Ketika ukuran data pelatihan (N) lebih kecil dari dimensionalitas data (d), $\boldsymbol{S_w^{-1}}$sering menjadi singular. Untuk menghindari masalah ini, pertama-tama kita dapat menerapkan PCA pada sampel pelatihan untuk mengurangi dimensionalitas data, lalu menerapkan LDA pada data yang ditransformasikan yang memiliki dimensionalitas lebih rendah. Gambar 3.24 menunjukkan tujuh Fisherface yang sesuai dengan tujuh nilai Eigen terbesar yang diperoleh melalui pelatihan pada gambar wajah yang terdapat dalam basis data ORL.

Gambar 3.24 Tujuh Fisherfaces yang sesuai dengan tujuh nilai Eigen terbesar yang diperoleh dari basis data wajah ORL.

Pengenalan wajah berbasis model

Teknik berbasis model mencoba memperoleh representasi gambar wajah yang tidak bergantung pada pose yang dapat memungkinkan pencocokan gambar wajah di berbagai pose. Skema ini biasanya memerlukan deteksi beberapa titik fiducial atau titik acuan di wajah (misalnya, sudut mata, ujung hidung, sudut mulut, daerah wajah yang homogen, dan dagu), yang mengarah pada peningkatan kompleksitas dibandingkan dengan teknik berbasis penampilan. Beberapa teknik berbasis model dapat digunakan untuk pengenalan wajah serta menghasilkan animasi wajah yang realistis. Model Face Bunch Graph akan dibahas di bagian ini, sedangkan skema pemodelan wajah yang lebih canggih akan dibahas.

Pencocokan Grafik Elastic Bunch

Skema Pencocokan Grafik Elastic Bunch (EBGM) merepresentasikan suatu sisi sebagai grafik gambar berlabel dengan setiap simpul menjadi titik fiducial atau titik acuan pada sisi tersebut. Sementara setiap simpul grafik diberi label dengan serangkaian koefisien Gabor (juga disebut jet) yang mencirikan informasi tekstur lokal di sekitar titik acuan, tepi yang menghubungkan dua simpul grafik diberi label berdasarkan jarak antara titik fiducial yang sesuai. Koefisien Gabor pada suatu lokasi dalam gambar dapat diperoleh dengan mengonvolusi gambar dengan filter Gabor 2D kompleks yang berpusat di lokasi tersebut. Dengan memvariasikan orientasi dan frekuensi filter Gabor, serangkaian koefisien atau jet Gabor dapat diperoleh. Penggunaan titik fiducial memungkinkan pembuatan grafik parsial bahkan jika sisi tersebut miring atau tertutup.

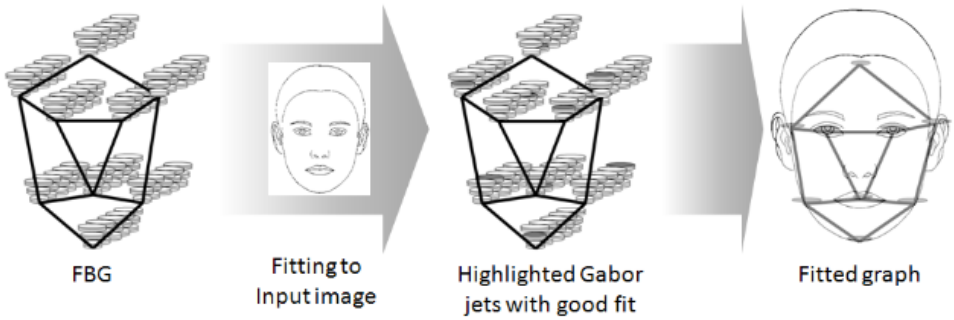
Model Face Bunch Graph (FBG) dapat dibangun dalam dua tahap dari set pelatihan gambar wajah dengan pose tertentu. Pada tahap pertama, perancang harus menandai titik fiducial yang diinginkan secara manual dan menentukan struktur geometris grafik gambar untuk satu (atau beberapa) gambar awal. Grafik gambar untuk gambar yang tersisa dalam set pelatihan dapat diperoleh secara semi-otomatis, dengan membandingkan gambar baru dengan grafik model (gambar yang telah ditandai) berdasarkan jet Gabor yang diekstraksi. Selama proses ini, intervensi manual diperlukan hanya jika titik fiducial diidentifikasi secara

tidak benar (lihat Gambar 3.25). Karena semua gambar pelatihan memiliki pose yang sama, grafik yang sesuai dengan gambar wajah ini akan memiliki struktur yang sama (yaitu, node merujuk ke titik fiducial yang identik). Proses yang sama dapat diulang untuk pose wajah yang berbeda (misalnya, tampilan depan, tampilan profil setengah dan penuh), dengan setiap pose memiliki struktur grafik yang berbeda.

Gambar 3.25 Menentukan grafik gambar untuk gambar wajah dengan pose yang berbeda. *Node diposisikan secara otomatis berdasarkan perbandingan jet Gabor yang diekstrak dari gambar yang diberikan dengan yang ada di grafik model. Kita dapat mengamati bahwa, secara umum, proses pemasangan menemukan titik fiducial dengan cukup akurat. Namun, kesalahan dapat terjadi seperti yang dapat diamati dalam kasus gambar wajah tengah di atas. Di gambar tengah, dagu tidak ditemukan secara akurat; lebih jauh, node paling kiri dan node di bawahnya idealnya harus ditempatkan di bagian atas dan bawah telinga, masing-masing.*

Pada tahap kedua, FBG diperoleh dari grafik gambar individual dengan menggabungkan satu set representatif grafik individual dalam struktur seperti tumpukan. Dengan demikian, setiap node dalam FBG diberi label oleh satu set jet Gabor yang mewakili variasi lokal dalam titik fiducial terkait di antara populasi pengguna dalam set pelatihan. Seperangkat jet yang sesuai dengan titik fiducial yang sama disebut sebagai kelompok. Misalnya, kelompok mata dapat mencakup jet dari mata terbuka, tertutup, mata pria dan wanita, dll. yang mencakup variasi dalam struktur mata setempat. Tepi antara dua simpul FBG diberi label berdasarkan jarak rata-rata antara simpul yang sesuai dalam set pelatihan. Biasanya, FBG terpisah dibangun untuk setiap pose dan korespondensi antara simpul grafik kelompok yang termasuk dalam pose yang berbeda ditentukan secara manual.

Dengan FBG, titik fiducial untuk gambar wajah baru ditemukan dengan memaksimalkan kesamaan antara grafik yang disesuaikan dengan gambar yang diberikan dan FBG dengan pose yang identik. Proses ini dikenal sebagai Elastic Bunch Graph Matching (EBGM) dan terdiri dari tiga langkah berikut:



Gambar 3.26 Grafik Kumpulan Wajah (FBG) berfungsi sebagai representasi umum wajah. Setiap tumpukan cakram mewakili sebuah jet. Dari sekumpulan jet yang melekat pada setiap simpul, hanya satu yang paling cocok yang dipilih untuk menghitung kesamaan dan jet tersebut ditunjukkan dengan bayangan abu-abu.

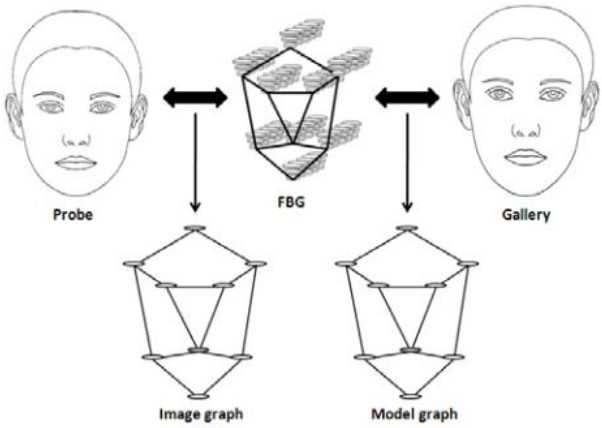
Temukan perkiraan posisi wajah dengan memindai gambar input secara kasar dengan FGB terkondensasi (grafik rata-rata yang diperoleh dengan mengambil jet Gabor rata-rata di setiap kumpulan). Hal ini dicapai dengan mengekstrak jet Gabor di beberapa lokasi diskrit dalam gambar yang diberikan dan membandingkannya dengan jet di FBG terkondensasi, sambil memperhitungkan struktur geometris FBG.

Pertajam posisi dan ukuran wajah dengan mencari gambar lagi dengan FBG penuh, yang ukuran dan rasio aspeknya divariasikan secara sistematis. Saat menghitung kesamaan antara jet Gabor dalam gambar yang diberikan dan sekumpulan jet di FBG, hanya jet FBG yang paling cocok dengan jet gambar yang diberikan yang dipertimbangkan. Tentukan lokasi titik fiducial secara tepat dengan memindahkan semua node secara lokal dan relatif satu sama lain untuk lebih mengoptimalkan kesamaan grafik.

Hasil dari algoritma EBGM adalah grafik gambar yang paling mewakili gambar yang diberikan berdasarkan model FBG yang tersedia. Gambar 3.26 menunjukkan Grafik Kumpulan Muka dengan tumpukan cakram (jet) di setiap node dan skema pemasangan grafik gambar ke gambar input. Untuk mencocokkan dua gambar muka, misalnya gambar probe dan galeri, grafik gambar pertama-tama dihitung dari kedua gambar ini. Grafik yang sesuai dengan gambar galeri terkadang juga disebut sebagai grafik model. Kesamaan antara grafik gambar dari gambar probe dan grafik model dihitung sebagai kesamaan rata-rata antara jet pada titik fiducial yang sesuai. Karena titik fiducial dan korespondensinya diketahui, kedua grafik dapat dicocokkan dengan sukses bahkan dengan beberapa node yang hilang. Akibatnya, skema EBGM lebih tangguh terhadap variasi pose daripada pendekatan berbasis tampilan.

Pengenalan wajah berbasis tekstur

Skema berbasis tampilan biasanya menggunakan nilai intensitas piksel mentah, yang cukup sensitif terhadap perubahan pencahayaan sekitar dan ekspresi wajah. Alternatifnya adalah menggunakan skema representasi fitur yang lebih tangguh yang mengkarakterisasi tekstur gambar menggunakan distribusi nilai piksel lokal. Scale Invariant Feature Transformation (SIFT) dan Local Binary Pattern (LBP) adalah dua skema yang paling terkenal untuk analisis tekstur lokal.

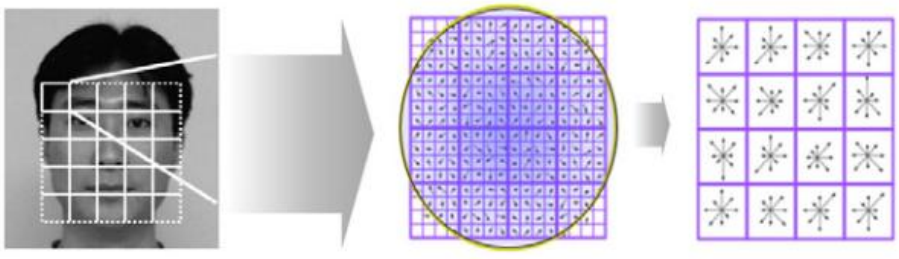


Gambar 3.27 Skema pembuatan grafik gambar dan model dari gambar probe dan galeri menggunakan Face Bunch Graph (FBG). Perhatikan bahwa ada kumpulan (kumpulan jet) di setiap simpul dalam FBG, tetapi hanya satu jet di setiap simpul dalam grafik gambar dan model.

Transformasi Fitur Invarian Skala

Transformasi Fitur Invarian Skala (SIFT) adalah salah satu skema representasi lokal paling populer yang digunakan dalam pengenalan objek. Perhitungan fitur SIFT terdiri dari dua tahap: (a) ekstraksi titik kunci, dan (b) perhitungan deskriptor di lingkungan lokal pada setiap titik kunci. Sama seperti titik fiducial dalam pendekatan berbasis model, titik kunci dapat digunakan untuk mencapai toleransi terhadap variasi pose.

Namun, jumlah titik kunci dalam SIFT bisa sangat besar (dalam urutan ratusan) dan menemukan korespondensi antara titik kunci dari dua gambar yang berbeda merupakan tugas yang menantang. Jika kita berasumsi bahwa gambar wajah kira-kira telah disejajarkan sebelumnya (misalnya, menggunakan lokasi mata), proses deteksi titik kunci dapat dilewati dan deskriptor dapat dibangun langsung dari seluruh gambar wajah. Deskriptor biasanya berupa histogram orientasi gradien dalam lingkungan lokal. Citra wajah biasanya dibagi dengan beberapa patch dan deskriptor SIFT dibuat dari setiap patch. Deskriptor akhir diperoleh dengan menggabungkan semua deskriptor dari semua patch. Gambar 3.28 menunjukkan diagram skematis dari proses pembuatan deskriptor SIFT di atas.



Gambar 3.28 Diagram skema konstruksi deskriptor SIFT. Proses deteksi titik kunci dapat dilewati jika gambar wajah telah disejajarkan sebelumnya.

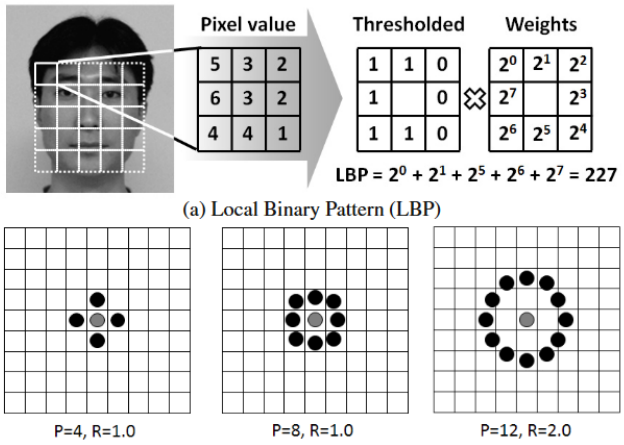
Pola Biner Lokal

Pola Biner Lokal (LBP) telah berhasil digunakan sebagai deskriptor tekstur lokal dalam pengenalan objek umum serta dalam pengenalan wajah. Fitur LBP biasanya diperoleh dari piksel gambar dari wilayah tetangga 3 x 3 (lihat Gambar 3.29(a)). Operator LBP dasar membandingkan 8 nilai intensitas piksel tetangga dengan nilai intensitas piksel pusat di wilayah tersebut dan merepresentasikan hasilnya sebagai string biner 8-bit. Kode biner ini selanjutnya dapat diubah menjadi angka desimal dengan menerapkan bobot pada setiap bit dan menghitung jumlahnya seperti yang ditunjukkan pada Gambar 3.29(a).

LBP Multiskala (MLBP) merupakan perluasan dari LBP dasar. Seperti yang diilustrasikan pada Gambar 3.29(b), MLBP memperkenalkan parameter radius R, yang berarti bahwa tetangga yang dibandingkan berjarak R piksel dari piksel pusat. Ada juga parameter lain P, yaitu jumlah titik pengambilan sampel di sepanjang lingkaran berjari-jari R. Jika titik pengambilan sampel berada di luar kisi piksel, interpolasi bilinear nilai piksel dapat diterapkan untuk memperoleh nilai intensitas titik pengambilan sampel.

Operator MLBP dengan parameter R dan P sering dilambangkan sebagai LBPP,R. Umumnya, MLBP dengan nilai P yang lebih besar memberikan informasi yang lebih terperinci tentang wilayah lokal. Akan tetapi, ketika P menjadi lebih besar, dimensi deskriptor juga meningkat. Operator MLBP dengan nilai R yang berbeda mengodekan struktur gambar lokal yang berbeda, mulai dari detail mikro hingga makro seperti yang diilustrasikan pada Gambar 3.30. Nilai R yang lebih kecil mengarah pada deteksi detail mikro, sedangkan nilai R yang lebih besar menyorot fitur makro.

Setelah pengodean LBP pada setiap piksel, gambar wajah dibagi menjadi beberapa jendela yang lebih kecil dan histogram pola biner lokal di setiap jendela dihitung. Jumlah bin dalam histogram adalah 8 dan 2P untuk LBP dasar dan MLBP, masing-masing. Vektor fitur global kemudian dihasilkan dengan menggabungkan histogram dari semua jendela individual dan menormalkan vektor akhir. Akhirnya, dua gambar wajah dapat dicocokkan dengan menghitung kesamaan (atau jarak) antara vektor fiturnya.



Gambar 3.29 Diagram skema perhitungan (a) Pola Biner Lokal (LBP) dan (b) LBP Multiskala. P dan R masing-masing merupakan jarak titik pengambilan sampel dari piksel pusat dan jumlah titik pengambilan sampel yang akan digunakan.

Gambar 3.30 Gambar Pola Biner Lokal (LBP) yang dikodekan pada skala yang berbeda. Dari kiri ke kanan: gambar asli; gambar yang dikodekan menggunakan operator LBP8,1, LBP8,3, dan LBP8,5, berturut-turut.

Evaluasi kinerja

Terdapat sejumlah basis data gambar wajah yang tersedia di domain publik. Tabel 3.1 merangkum beberapa basis data gambar wajah yang representatif di domain publik. Sebagian besar studi pengenalan wajah menggunakan pilihan basis data dan pengaturan eksperimen mereka sendiri. Bahkan untuk basis data yang sama dan algoritma pengenalan yang sama, akurasi pengenalan dapat bervariasi karena faktor-faktor seperti protokol evaluasi yang berbeda (misalnya, pembagian probe dan set galeri), skema deteksi wajah dan normalisasi gambar yang berbeda, dan pemilihan parameter yang berbeda (misalnya, dimensionalitas subruang). Oleh karena itu, sulit untuk membandingkan hasil eksperimen yang dipublikasikan.

Tabel 3.1 Basis data citra wajah.

Menghadapi DB	Subjek	Gambar	Variasi termasuk
ORL	40	400	I,e,t
Yale	15	165	P,e
AR	126	4,000	e,i,o
MIT	16	432	P,i,s
UMIST	20	564	P
CMU PIE	68	41,368	P,i,e
XM2VTS	295	1,180 (vidio)	P,i,t
FERET	10,465	14,051	P,i,e,t
FRGC (v.2.0)	568	36,818	I,e,t
MBGC	522	9,307	S,i,o
FG-NET	82	1002	P,i,e,t
MORPH	20,569	78,207	T

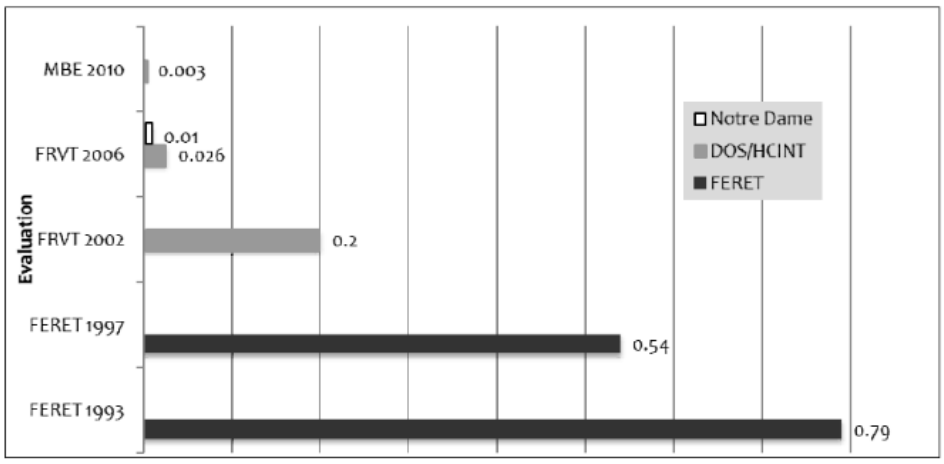
p: pose; i: iluminasi; e: ekspresi; o: oklusi; s: skala; t: interval waktu (penuaan).

Dalam upaya untuk membandingkan akurasi berbagai teknik pengenalan wajah pada basis data citra wajah umum dan skala besar, beberapa kompetisi pengenalan wajah telah diadakan. Program Teknologi Pengenalan Wajah (FERET) yang berlangsung dari tahun 1993 hingga 1997 merupakan upaya pertama untuk membandingkan berbagai teknik pengenalan

wajah dengan peserta dari berbagai universitas. Setelah FERET, Face Recognition Vendor Test (FRVT) dan Face Recognition Grand Challenge (FRGC) melanjutkan uji perbandingan dengan peserta dari industri dan akademisi.

Dalam FRVT 2002, algoritme terbaik mencapai akurasi identifikasi peringkat-1 sekitar 70% dalam pose hampir frontal dan kondisi pencahayaan normal pada basis data besar (121.589 gambar dari 37.437 subjek). Evaluasi FRVT 2006 dilakukan untuk skenario verifikasi dan sistem pengenalan wajah terbaik memiliki False Reject Rate (FRR) sebesar 0,01 pada False Accept Rate (FAR) sebesar 0,001 untuk gambar 2D beresolusi tinggi (sekitar 400 piksel jarak antar pupil (IPD)) dan gambar 3D. Evaluasi terkini seperti Multiple Biometric Evaluation 2010 menunjukkan bahwa kinerja sistem pengenalan wajah telah meningkat dibandingkan dengan pengujian sebelumnya.

Gambar 3.31 menunjukkan peningkatan kinerja pengenalan wajah dari tahun 1993 hingga 2006 dalam hal Tingkat Penolakan Palsu pada Tingkat Penerimaan Palsu yang tetap dalam mode verifikasi.



Gambar 3.31 Peningkatan akurasi pengenalan wajah dari tahun 1993 hingga 2010 dalam hal False Reject Rate pada False Accept Rate yang tetap dalam mode verifikasi. Perhatikan bahwa basis data citra wajah Notre Dame dan DOS/HCINT tidak tersedia dalam domain publik.

Baru-baru ini, ada upaya untuk mengumpulkan sejumlah besar citra wajah dari Internet guna mengevaluasi kinerja pengenalan wajah. Labeled Faces in the Wild (LFW) dan kumpulan citra wajah dari Facebook adalah contohnya. Set data LFW terdiri dari lebih dari 13.233 citra wajah dari 5.947 orang; 1.680 subjek memiliki dua atau lebih citra yang dapat digunakan untuk mengevaluasi algoritme pengenalan wajah. Saat ini, 22 algoritme berbeda telah dievaluasi pada set data LFW dan hasil evaluasinya dipublikasikan di situs web resmi1.

3.5 PENANGANAN VARIASI POSE, PENCAHAYAAN, DAN EKSPRESI

Variasi pose merupakan salah satu sumber utama penurunan kinerja dalam pengenalan wajah. Wajah merupakan objek 3D yang tampak berbeda tergantung dari arah

mana wajah tersebut diambil. Dengan demikian, ada kemungkinan bahwa gambar subjek yang sama yang diambil dari dua sudut pandang yang berbeda mungkin tampak lebih berbeda (variasi intra-pengguna) daripada gambar dua subjek berbeda yang diambil dari sudut pandang yang sama (variasi antar-pengguna).

Variasi pencahayaan atau iluminasi merupakan sumber penurunan kinerja lainnya. Karena wajah merupakan objek 3D, sumber pencahayaan yang berbeda dapat menghasilkan berbagai kondisi dan bayangan iluminasi. Telah ada upaya untuk mengembangkan fitur wajah yang tidak berubah saat terjadi perubahan pencahayaan. Alternatif lainnya adalah mempelajari dan mengompensasi variasi pencahayaan menggunakan pengetahuan sebelumnya tentang sumber pencahayaan berdasarkan data pelatihan.

Untuk mengatasi masalah tersebut di atas, sistem pengenalan wajah berbasis gambar 3D telah dikembangkan. Metode pengenalan wajah 3D menggunakan geometri permukaan wajah. Tidak seperti pengenalan wajah 2D, pengenalan wajah 3D kuat terhadap variasi pose dan pencahayaan karena invariansi bentuk 3D terhadap variasi ini. Probe biasanya berupa gambar 2.5D dan galeri dapat berupa gambar 2.5D atau model 3D. Identifikasi dapat dilakukan antara dua gambar rentang (kedalaman) atau antara gambar 2D dan model wajah 3D.

Ekspresi wajah merupakan fenomena inheren yang menyebabkan variasi intra-kelas yang besar. Ada beberapa pendekatan berbasis fitur lokal dan pendekatan berbasis model 3D yang dirancang untuk menangani masalah ekspresi. Di sisi lain, pengenalan ekspresi wajah itu sendiri merupakan area penelitian aktif di bidang interaksi dan komunikasi manusia-komputer.

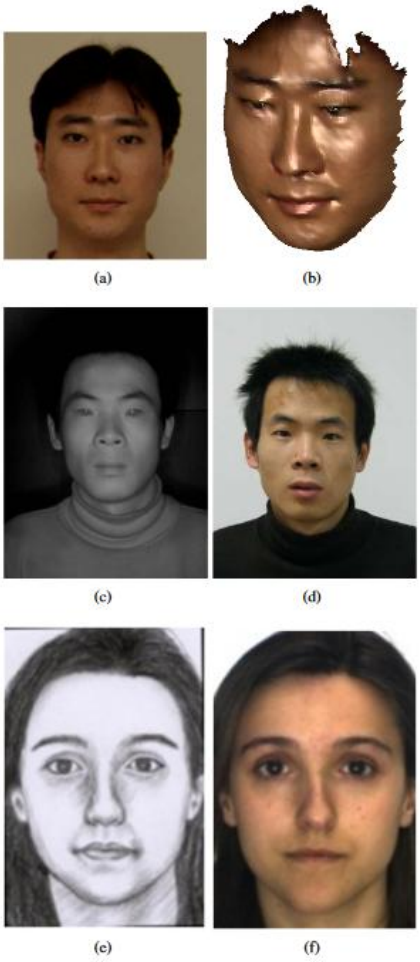
Sumber penurunan kinerja lain dalam pengenalan wajah adalah oklusi. Citra wajah sering kali tampak tertutup oleh objek lain atau oleh wajah itu sendiri (yaitu, oklusi diri), terutama dalam video pengawasan. Sebagian besar mesin pengenalan wajah komersial menolak citra tersebut ketika mata tidak dapat dideteksi. Metode berbasis fitur lokal telah diusulkan untuk mengatasi masalah oklusi.

Pengenalan wajah heterogen

Pengenalan wajah heterogen mengacu pada pencocokan citra wajah di berbagai format citra yang memiliki karakteristik pembentukan citra yang berbeda. Contohnya termasuk pencocokan citra 2D dengan model 3D, citra dari spektrum tampak dengan citra inframerah, foto tersangka dengan sketsa forensik, atau foto pindaian dengan citra yang diperoleh menggunakan kamera digital biasa. Gambar 3.32 menunjukkan contoh gambar heterogen yang umum ditemui dalam pengenalan wajah. Karena heterogenitas dapat meningkatkan variabilitas intra-kelas, perhatian khusus perlu diberikan dalam pengenalan wajah heterogen.

Skenario yang paling umum ditemui dalam pengenalan wajah heterogen melibatkan basis data galeri dengan gambar diam 2D dari spektrum tampak dan gambar probe dari beberapa modalitas alternatif (misalnya inframerah, sketsa, atau 3D). Hal ini karena adanya basis data wajah lama (misalnya, foto SIM, catatan foto tersangka dari penegak hukum, basis data Visa Departemen Luar Negeri) yang berisi foto sebagian besar penduduk di AS serta di

sebagian besar negara maju lainnya. Sayangnya, ada banyak skenario di mana gambar probe bukan foto. Misalnya, dalam penegakan hukum, ketika tidak ada gambar wajah tersangka yang tersedia, sketsa forensik dapat dikembangkan melalui deskripsi verbal tentang penampilan tersangka. Untuk mengidentifikasi subjek dalam skenario seperti itu, algoritma khusus untuk pengenalan wajah heterogen harus digunakan.



Gambar 3.32 Contoh pencocokan citra wajah heterogen.

Baris teratas sesuai dengan skenario saat foto tersangka 2D yang ditunjukkan pada (a) dicocokkan dengan model 3D yang ditunjukkan pada (b). Baris tengah adalah contoh pencocokan citra 2D yang direkam dalam spektrum inframerah dekat (gambar (c)) dengan foto tersangka 2D yang direkam dalam spektrum tampak (gambar (d)). Baris terbawah sesuai dengan pencocokan sketsa forensik yang ditunjukkan pada (e) dengan foto tersangka 2D yang ditunjukkan pada (f).

Kumpulan solusi untuk pengenalan wajah heterogen dapat diorganisasikan ke dalam tiga kategori:

a) **Metode sintesis**: Metode sintesis berupaya menghasilkan foto sintetis yang terlihat dari format gambar wajah alternatif yang tersedia. Setelah gambar wajah yang terlihat disintesis, gambar tersebut dapat dicocokkan menggunakan algoritma pengenalan wajah standar. Solusi sintesis untuk pengenalan wajah heterogen adalah metode generatif dan biasanya menggunakan teknik seperti penyematan linier lokal atau medan acak Markov.

b) **Metode berbasis fitur**: Metode berbasis fitur mengodekan gambar wajah dari kedua modalitas menggunakan deskriptor fitur yang sebagian besar tidak berubah terhadap perubahan antara kedua domain. Misalnya, pola biner lokal dan deskriptor fitur SIFT telah terbukti stabil antara sketsa dan foto yang terlihat, serta gambar wajah inframerah dekat dan foto yang terlihat. Setelah gambar wajah dari kedua format gambar direpresentasikan menggunakan deskriptor fitur, metode ekstraksi fitur seperti LDA dapat digunakan untuk meningkatkan kemampuan diskriminatif representasi. Tahap pencocokan metode berbasis fitur dilakukan dengan mengukur jarak atau kesamaan antara representasi vektor fitur dari dua gambar wajah.

c) **Metode kesamaan prototipe**: Metode kesamaan prototipe merepresentasikan gambar wajah sebagai vektor kesamaan dengan gambar dalam basis data prototipe. Misalkan kita perlu mencocokkan gambar probe berformat A dengan gambar galeri berformat B. Basis data prototipe terdiri dari kumpulan subjek yang gambar wajahnya tersedia dalam format A dan format B. Prototipe dianalogikan dengan set pelatihan - dalam hal ini, prototipe membantu memperkirakan distribusi wajah. Gambar probe dapat dicocokkan dengan gambar berformat A dari basis data prototipe untuk menghasilkan vektor kesamaan. Vektor kesamaan lainnya dapat diperoleh dengan mencocokkan gambar galeri dengan gambar berformat B dalam basis data prototipe. Kesamaan ini dapat diukur menggunakan representasi berbasis tekstur (misalnya, LBP, SIFT) dari gambar wajah. Gambar probe dan galeri dapat dicocokkan dengan membandingkan langsung kedua vektor kesamaan. Analisis diskriminan linear juga dapat diterapkan pada vektor kesamaan untuk meningkatkan akurasi pengenalan. Keuntungan dari pendekatan kesamaan prototipe adalah bahwa representasi fitur mungkin berbeda untuk format gambar probe dan galeri. Properti ini berguna dalam skenario seperti pencocokan 3D ke 2D, di mana deskriptor fitur umum tidak ada di antara kedua format gambar.

Pemodelan wajah

Tujuan pemodelan wajah adalah untuk mengodekan properti gambar wajah (misalnya, bentuk, penampilan, penuaan) menggunakan serangkaian parameter yang ringkas yang memungkinkan interpretasi gambar wajah baru dengan menghasilkan gambar sintetis yang semirip mungkin dengan gambar yang diberikan. Dengan demikian, representasi parametrik tidak hanya memungkinkan perbandingan antara gambar wajah yang berbeda, tetapi juga dapat digunakan untuk menghasilkan animasi wajah yang realistis. Model Penampilan Aktif (AAM), Model Bentuk Aktif (ASM), dan model yang dapat diubah bentuk adalah teknik pemodelan wajah yang paling populer.

Model Penampilan Aktif

Model Penampilan Aktif (AAM) adalah model statistik penampilan wajah yang dihasilkan dengan menggabungkan variasi bentuk dan tekstur. Diberikan serangkaian gambar wajah pelatihan $I_1, I_2, \ldots, I_N$, AAM dapat dibangun sebagai berikut. Biarkan p_i mewakili vektor titik fiducial dalam gambar I_i. Korespondensi yang tepat dari titik-titik

fiducial diperlukan di semua gambar pelatihan N. Dengan menerapkan PCA ke set pelatihan titik-titik fiducial $p_1, p_2, \ldots, p_N$ setiap p_j dapat diperkirakan sebagai

$$\mathbf{p_j} = \mathbf{p_\mu} + \mathbf{E_s}\boldsymbol{\omega_{s_j}} \tag{3.10}$$

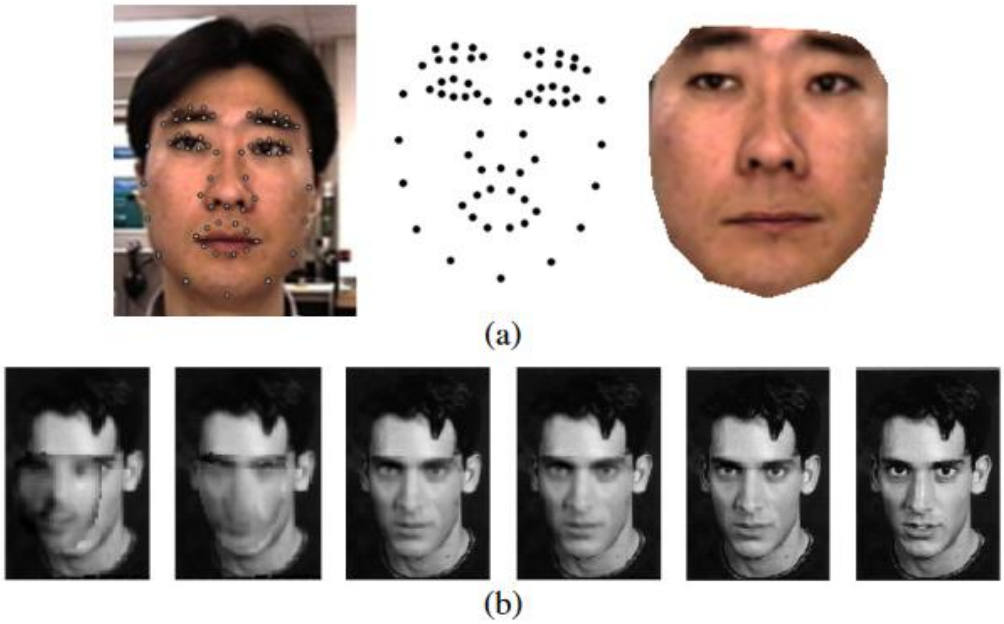
di mana $\mathbf{p_\mu}$ adalah bentuk rata-rata, $\mathbf{E_s}$ adalah matriks vektor Eigen (yang mewakili mode variasi ortogonal) yang diperoleh dengan menerapkan PCA pada set pelatihan, dan $\boldsymbol{\omega_{s_j}}$ adalah satu set parameter bentuk. Untuk membangun model tekstur, setiap gambar pelatihan dilengkungkan sehingga titik fiducialnya cocok dengan bentuk rata-rata. Biarkan $\mathbf{g}_i$ mewakili tekstur wajah yang diekstraksi dari gambar I_i, yaitu, intensitas piksel vektor setelah melengkungkan I_i agar sesuai dengan bentuk rata-rata. Model tekstur didefinisikan mirip dengan model bentuk sebagai

$$\mathbf{g_j} = \mathbf{g_\mu} + \mathbf{E_g}\boldsymbol{\omega_{g_j}} \tag{3.10}$$

di mana $\mathbf{g_\mu}$ adalah tekstur rata-rata, $\mathbf{E_g}$ adalah matriks vektor Eigen yang diperoleh dengan menerapkan PCA ke set pelatihan $\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_N}$dan $\boldsymbol{\omega_{g_j}}$ adalah satu set parameter tekstur. Parameter bentuk dan tekstur dapat dipertimbangkan bersama-sama dan setiap gambar wajah I_i dapat direpresentasikan sebagai $\boldsymbol{\omega_j} = (\boldsymbol{\omega_{s_j}}, \boldsymbol{\omega_{g_j}})$. Sekarang masalahnya adalah untuk menemukan vektor parameter bentuk dan tekstur terbaik $\boldsymbol{\omega_j}$ yang meminimalkan perbedaan antara gambar yang diberikan I_j^m dan gambar sintetis I_j yang dihasilkan oleh model saat ini yang didefinisikan oleh $\boldsymbol{\omega_j}$. Ini biasanya dicapai melalui skema optimasi yang tepat. Parameter model $\boldsymbol{\omega_j}$ dan $\boldsymbol{\omega_k}$ yang berasal dari dua gambar wajah yang berbeda I_i dan I_k, masing-masing, dapat langsung dicocokkan untuk menentukan kesamaan antara I_i dan I_k. Gambar 3.33 menunjukkan contoh bagaimana teknik AAM membagi citra wajah menjadi komponen bentuk dan tekstur serta proses penyesuaian model.

Model Morphable

Model Morphable (MM) menggunakan titik-titik 3D (baik informasi lokasi maupun kedalaman tentang titik-titik fiducial) untuk merepresentasikan bentuk wajah 3D dan tekstur warna (intensitas piksel dalam saluran merah, hijau, dan biru) untuk merepresentasikan tampilan wajah. Sebaliknya, AAM biasanya hanya menggunakan lokasi titik-titik fiducial dan intensitas piksel skala abu-abu. Oleh karena itu, model morphable dapat dianggap sebagai versi 3D dari AAM dengan tekstur warna. Karena model morphable menggunakan informasi 3D, prosedur pemasangannya lebih rumit daripada AAM dengan pertimbangan tambahan panjang fokus, intensitas cahaya sekitar, intensitas dan sudut cahaya terarah, kontras warna, serta perolehan dan offset saluran warna. Gambar 3.34 menunjukkan contoh pemasangan model morphable ke gambar 2D pada berbagai pose.



Gambar 3.33 Contoh pelatihan dan pemasangan AAM.

(a) Gambar pelatihan dibagi menjadi bentuk dan tekstur yang dinormalisasi bentuk. (b) Contoh iterasi pemasangan AAM.

Model Penuaan Wajah

Perubahan yang berkaitan dengan penuaan pada wajah terwujud dalam sejumlah cara berbeda: (a) kerutan dan bintik-bintik, (b) penurunan dan penambahan berat badan, dan (c) perubahan bentuk primitif wajah (misalnya, mata, pipi, atau mulut yang kendur). Semua variasi yang berkaitan dengan penuaan ini menurunkan kinerja pengenalan wajah. Cara sederhana untuk menangani variasi penuaan adalah dengan memperbarui templat wajah dalam basis data secara berkala.

Namun, ini hanya mungkin dilakukan dalam beberapa aplikasi verifikasi wajah yang terkontrol. Meskipun variasi penuaan berdampak negatif pada akurasi pengenalan wajah, masalah pengenalan wajah yang tidak bergantung pada usia belum dipelajari secara ekstensif karena dua alasan. Pertama, variasi pose dan pencahayaan umumnya dianggap sebagai faktor yang lebih kritis yang menurunkan kinerja pengenalan wajah. Kedua, hingga saat ini, tidak ada basis data domain publik yang tersedia untuk mempelajari efek penuaan.

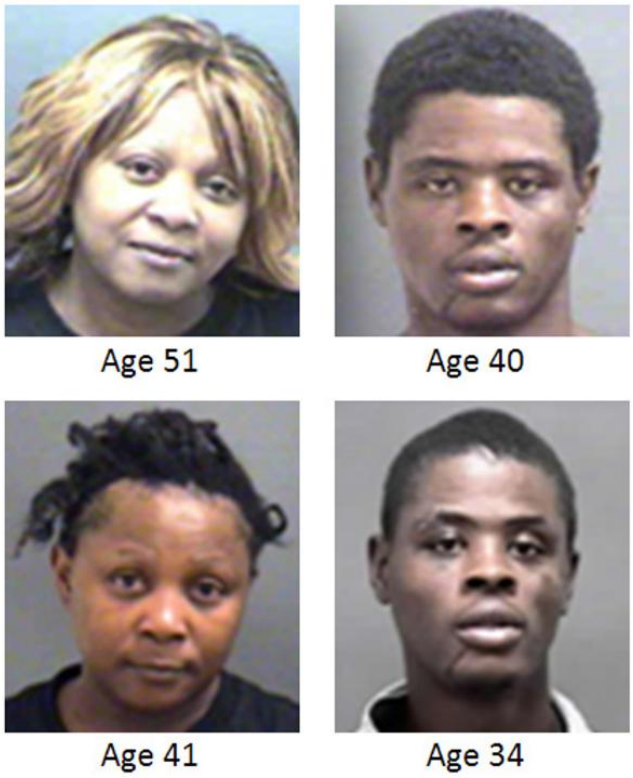
Salah satu pendekatan yang berhasil untuk pengenalan wajah yang tidak bergantung pada usia adalah dengan membangun model generatif 2D atau 3D untuk penuaan wajah. Model penuaan dapat digunakan untuk mengompensasi proses penuaan dalam pencocokan wajah atau estimasi usia. Metode-metode ini pertama-tama mengubah citra probe ke usia yang sama dengan citra galeri menggunakan model penuaan yang terlatih untuk mengompensasi efek usia. Sementara metode berbasis model telah terbukti efektif dalam pengenalan wajah yang tidak bergantung pada usia, metode ini memiliki beberapa keterbatasan. Pertama, konstruksi model penuaan wajah sulit dan model yang dibangun mungkin tidak mewakili proses penuaan dengan baik.

Gambar 3.34 Contoh pemasangan model yang dapat diubah bentuknya.

Baris atas: Parameter awal. Baris tengah: Hasil pemasangan, ditampilkan di atas gambar masukan. Baris bawah: Gambar masukan. Kolom kelima adalah contoh pemasangan yang buruk. Gambar berasal dari [4].

Karena proses penuaan wajah agak rumit dan jumlah citra pelatihan seringkali sangat terbatas, konstruksi model penuaan memerlukan penggunaan asumsi parametrik yang kuat yang seringkali tidak realistis dalam skenario pengenalan wajah di dunia nyata. Kedua, informasi tambahan dalam bentuk usia sebenarnya dari wajah-wajah dalam set pelatihan dan lokasi titik-titik penting pada setiap citra wajah diperlukan untuk membangun model penuaan. Informasi ini tidak selalu tersedia. Kendala lebih lanjut pada set pelatihan adalah bahwa gambar harus diambil dalam kondisi terkendali (misalnya, pose frontal, pencahayaan normal, ekspresi netral).

Sayangnya, kendala tersebut tidak mudah dipenuhi dalam praktik, terutama dalam skenario di mana gambar wajah yang dibandingkan mengalami perubahan signifikan tidak hanya dalam penuaan, tetapi juga dalam pose, pencahayaan, dan ekspresi. Untuk mengatasi keterbatasan model penuaan generatif, pendekatan berdasarkan model diskriminatif juga telah diusulkan. Dalam model penuaan diskriminatif, gambar wajah direpresentasikan oleh serangkaian fitur yang kuat (misalnya, MLBP), kemudian diproyeksikan ke beberapa subruang tempat variasi penuaan dikompensasi. Contoh model penuaan diskriminatif adalah penggunaan piramida orientasi gradien untuk representasi fitur, dikombinasikan dengan penggunaan mesin vektor pendukung untuk memverifikasi wajah di seluruh perkembangan usia. Gambar 3.35 menunjukkan beberapa contoh pasangan gambar wajah yang dapat berhasil dicocokkan menggunakan model penuaan generatif atau diskriminatif yang disebutkan di atas.



Gambar 3.35 Contoh pasangan citra wajah pada usia berbeda yang diambil dari dua subjek berbeda. Pencocok komersial terkemuka gagal mencocokkan pasangan ini, tetapi model penuaan generatif atau diskriminatif berhasil mencocokkan pasangan ini. Baris atas dan bawah masing-masing sesuai dengan citra probe dan galeri.

Ringkasan

Bab ini mengulas berbagai pendekatan pengenalan wajah dengan penekanan pada pencocokan gambar diam 2D yang diambil dalam spektrum tampak. Meskipun telah terjadi peningkatan yang stabil dalam kinerja pengenalan wajah selama dua dekade terakhir, beberapa tantangan tetap ada karena variasi intra-kelas yang besar dan variasi antar-kelas yang kecil yang disebabkan oleh variasi pose dan pencahayaan, ekspresi, oklusi, penuaan, dan representasi data gambar wajah yang tidak kuat. Sementara sistem pengenalan wajah 3D telah dikembangkan untuk mengatasi masalah pose dan pencahayaan, sejumlah faktor (misalnya, biaya tinggi dan keberadaan basis data wajah lama yang besar dalam domain 2D) telah menghambat penerapan praktis sistem pengenalan wajah 3D. Teknik penginderaan canggih untuk menangkap gambar beresolusi lebih tinggi dalam beberapa spektrum, teknik deteksi wajah yang dapat menangani perubahan pose, dan skema representasi dan pencocokan yang kuat sangat penting untuk lebih meningkatkan akurasi sistem pengenalan wajah.

BAB 4
PENGENALAN IRIS

"[Iris] terdiri dari ligamen pektinat yang melekat pada jalinan kusut yang memperlihatkan garis-garis, prosesus siliaris, kripta, cincin, alur, korona, terkadang bintik-bintik, pembuluh darah, dan fitur lainnya". Tekstur iris yang kaya dapat digunakan sebagai isyarat biometrik untuk pengenalan orang. Kekayaan dan variabilitas yang diamati dalam tekstur iris disebabkan oleh pengelompokan beberapa entitas anatomi yang menyusun strukturnya. Karena adanya informasi yang khas pada beberapa skala, pendekatan pemrosesan sinyal berbasis wavelet umumnya digunakan untuk mengekstraksi fitur dari iris. Salah satu pendekatan paling populer untuk pengenalan iris menghasilkan kode biner untuk mewakili dan mencocokkan pasangan iris.

Pertama, rutinitas segmentasi digunakan untuk mendeteksi daerah iris dalam gambar okular yang ditangkap oleh kamera. Selanjutnya, metode normalisasi geometrik digunakan untuk mengubah daerah iris yang hampir melingkar menjadi entitas persegi panjang. Kemudian, entitas persegi panjang ini dikonvolusikan dengan filter Gabor yang menghasilkan respons kompleks, dan informasi fase respons berikutnya dikuantisasi menjadi kode biner, yang umumnya disebut sebagai kode iris. Terakhir, jarak Hamming digunakan untuk membandingkan dua kode iris dan menghasilkan skor kecocokan, yang digunakan untuk pengenalan biometrik. Bab ini membahas aspek-aspek penting dari sistem pengenalan iris yang umum.

4.1 PENDAHULUAN

Pemanfaatan daerah mata sebagai ciri biometrik telah mendapatkan dorongan, terutama karena kemajuan signifikan yang dibuat dalam pengenalan iris sejak tahun 1993. Daerah mata wajah manusia terdiri dari mata dan struktur di sekitarnya seperti kulit wajah, alis, dan pangkal hidung (Gambar 4.1).

Meskipun berbagai komponen mata telah diusulkan sebagai indikator biometrik misalnya, iris, retina, dan pembuluh darah konjungtiva, irislah yang telah dipelajari secara ekstensif dalam literatur biometrik dan digunakan dalam sistem biometrik skala besar. Iris adalah organ internal mata yang terletak tepat di belakang kornea dan di depan lensa. Fungsi utama iris adalah mengatur jumlah cahaya yang masuk ke mata dengan melebarkan atau menyempitkan lubang kecil di dalamnya yang disebut pupil. Iris menyempitkan pupil saat pencahayaan sekitar tinggi dan melebarkannya saat pencahayaan rendah. Iris adalah struktur berlapis-lapis dan penampang iris memperlihatkan lapisan-lapisan berikut: Lapisan posterior di bagian belakang, yang tebalnya dua sel, mengandung sel-sel epitel berpigmen tebal, sehingga tidak dapat ditembus cahaya. Lapisan otot di atasnya terdiri dari otot sfingter dan dilator yang menyempitkan dan melebarkan pupil. Lapisan stroma, yang terletak di atas otot, terdiri dari jaringan ikat kolagen (tersusun dalam konfigurasi seperti lengkung) dan pembuluh darah (tersusun sepanjang arah radial).

Lapisan batas anterior adalah lapisan paling depan dan memiliki kepadatan kromatofora (yaitu, sel yang mengandung pigmen) yang lebih tinggi dibandingkan dengan lapisan stroma.

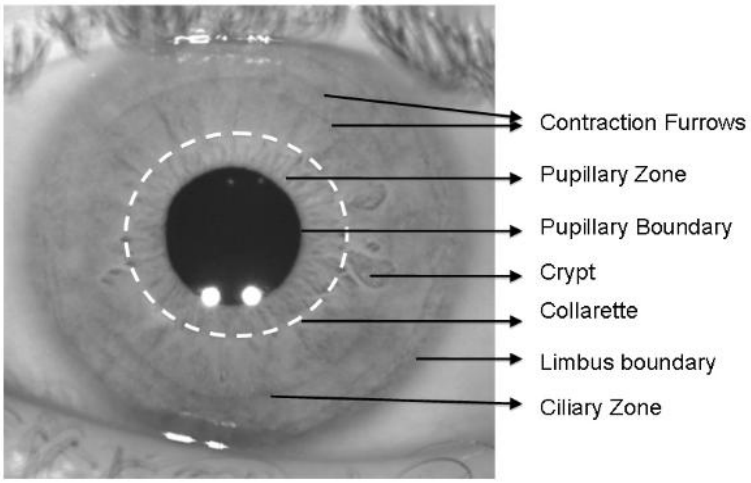
Gambar 4.1 Daerah Ocular Wajah Manusia

Gambar 4.1 Daerah okular wajah manusia meliputi mata, alis, pangkal hidung, dan kulit wajah. Iris adalah struktur berwarna yang terletak di daerah annular mata dan dibatasi oleh pupil (lubang gelap di mata) dan sklera (bagian putih mata). Bila dilihat secara rinci, bahkan iris kiri dan iris kanan seseorang menunjukkan perbedaan signifikan dalam teksturnya, meskipun beberapa kesamaan global dapat diamati. Perlu dicatat bahwa sistem pengenalan iris yang umum tidak menggunakan warna iris untuk pengenalan manusia.

Bagian anterior iris - yang secara kolektif terdiri dari otot, stroma, dan lapisan tepi - merupakan bagian iris yang paling terlihat. Oleh karena itu, bagian ini dapat dicitrakan oleh kamera dan menjadi fokus semua sistem pengenalan iris otomatis. Gambar 4.2 menunjukkan citra iris sebagaimana dilihat oleh kamera inframerah dekat. Iris, dari perspektif ini, tampak sebagai entitas melingkar yang dibatasi oleh batas pupil (yang memisahkannya dari pupil gelap) dan batas limbus (yang memisahkannya dari sklera putih). Citra iris dibagi menjadi dua zona: zona pupil sentral dan zona silia di sekitarnya. Kedua zona ini dibagi oleh garis lengkung zigzag melingkar yang dikenal sebagai collarette. Banyak struktur tidak beraturan seperti lubang muncul terutama di wilayah sekitar collarette. Struktur ini disebut kripta (kripta Fuchs) dan memungkinkan cairan masuk dan keluar iris dengan cepat selama pelebaran dan kontraksi pupil. Di dekat bagian luar zona silia, garis-garis konsentris dapat terlihat, terutama pada kasus iris yang berpigmen gelap. Garis-garis ini menjadi lebih dalam saat pupil melebar dan disebut alur kontraksi. Di zona pupil, alur radial terlihat.

Pengumpulan struktur yang disebutkan di atas memberikan tekstur yang kaya pada iris. Istilah tekstur menunjukkan karakteristik gambar dalam hal homogenitas, kekasaran, keteraturan, arah, dll. Literatur biometrik menunjukkan bahwa iris menunjukkan keragaman substansial dalam teksturnya di seluruh populasi. Keunikan setiap iris diasumsikan sebagai konsekuensi dari morfogenesis acak dari relief teksturnya selama pertumbuhan prenatal. Bahkan iris dari kembar monozigot menunjukkan perbedaan dalam teksturnya, dengan demikian menunjukkan bahwa pola-pola ini ditentukan secara epigenetik oleh peristiwa acak selama perkembangan yang memengaruhi morfogenesis jaringan. Dengan menggunakan terminologi yang dikembangkan dalam Bab 1, tekstur iris sebagian besar merupakan sifat

fenotipik dengan penetrasi genetik terbatas. Warna iris terutama ditentukan oleh pigmentasi yang ada di dalamnya. Pigmentasi itu sendiri dikendalikan oleh jumlah butiran melanin - faktor yang ditentukan secara genetik. Namun, faktor lain, seperti kepadatan sel stroma, juga dapat memengaruhi warna iris. Seperti yang akan dijelaskan nanti, warna iris tidak memainkan peran penting dalam sistem pengenalan iris. Detail tekstur yang ada di bagian anterior irislah yang berguna untuk pengenalan.

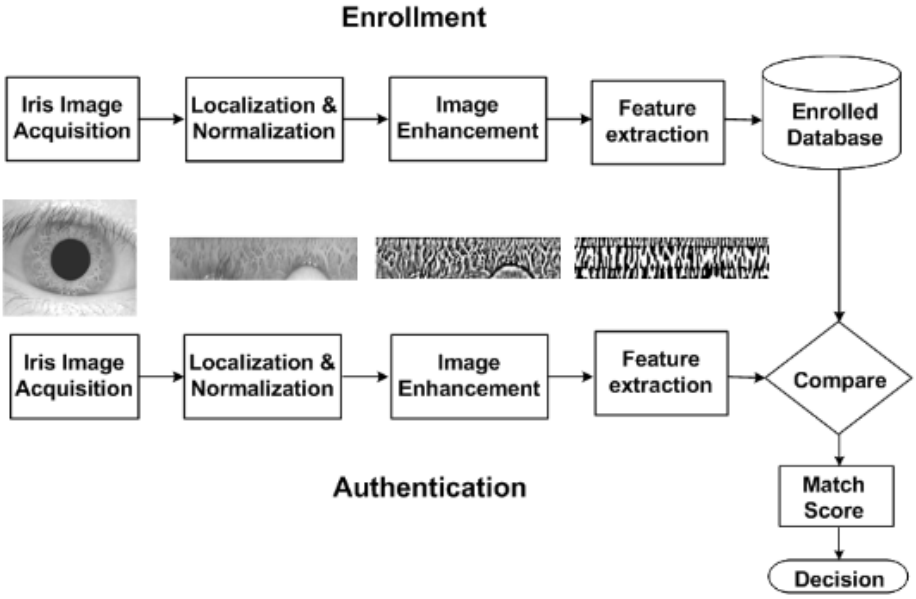


Gambar 4.2 Anatomi Iris

Gambar 4.2 Anatomi iris seperti yang diamati oleh kamera inframerah dekat yang ditempatkan di depan mata. Tekstur iris yang kaya disebabkan oleh bagian anteriornya yang terdiri dari otot, stroma, dan lapisan tepi anterior. Ketika lapisan tepi anterior surut, kolarette menjadi terlihat sebagai garis zig-zag yang memisahkan zona silia dari zona pupil. Struktur tidak beraturan seperti kawah yang disebut kripta sering diamati ketika lapisan anterior menipis, sehingga memperlihatkan lapisan posterior yang sangat berpigmen dan jauh lebih gelap.

4.2 DESAIN SISTEM PENGENALAN IRIS

Sistem pengenalan iris dapat dilihat sebagai sistem pencocokan pola yang tujuannya adalah membandingkan dua iris dan menghasilkan skor kecocokan yang menunjukkan tingkat kesamaan atau ketidaksamaannya. Dengan demikian, sistem pengenalan iris yang umum memiliki empat modul berbeda: modul akuisisi, segmentasi, normalisasi, dan pengodean/pencocokan. Gambar 4.3 menunjukkan aliran informasi dalam sistem pengenalan iris yang umum.



Gambar 4.3 Diagram Blok Sistem Pengendalian Iris

Gambar 4.3 Diagram blok sistem pengenalan iris. Kinerja pencocokan sistem pengenalan iris dapat dipengaruhi oleh keakuratan modul segmentasi, yang mendeteksi iris dan menetapkan luas spasialnya dalam gambar daerah mata.

1. **Akuisisi:** Peran modul akuisisi adalah untuk memperoleh gambar mata 2D menggunakan kamera CCD monokrom yang peka terhadap jangkauan inframerah dekat (NIR) dari spektrum elektromagnetik. Sumber cahaya NIR eksternal, yang sering kali ditempatkan bersama dengan sistem akuisisi, digunakan untuk menerangi iris. Sebagian besar sistem pengenalan iris mengharuskan peserta untuk bersikap kooperatif dan mendekatkan mata mereka ke kamera. Sistem ini biasanya menangkap serangkaian gambar mata dan, berdasarkan skema evaluasi kualitas, hanya menyimpan beberapa gambar yang dianggap memiliki informasi tekstur iris yang cukup untuk diproses lebih lanjut.
2. **Segmentasi:** Modul segmentasi melokalisasi batas spasial iris pada citra mata dengan mengisolasinya dari struktur lain yang ada di sekitarnya. Struktur ini meliputi sklera, pupil, kelopak mata, dan bulu mata. Biasanya, segmentasi dilakukan dengan mendeteksi batas dalam dan luar iris (umumnya disebut batas pupil dan batas limbus), serta kelopak mata dan bulu mata yang dapat mengganggu kontur melingkar batas limbus. Operator integro-diferensial, yang dijelaskan kemudian, umumnya digunakan untuk mendeteksi batas iris, meskipun, baru-baru ini, penggunaan kontur aktif telah diusulkan untuk memperhitungkan kasus ketika batas tidak dapat direpresentasikan sebagai penampang kerucut sederhana seperti lingkaran atau elips. Segmentasi iris merupakan komponen penting dari setiap sistem biometrik iris; ketidakakuratan dalam melokalisasi iris dapat sangat memengaruhi akurasi pencocokan sistem, sehingga merusak kegunaannya.

3. **Normalisasi:** Setelah batas dalam dan luar iris diperkirakan, skema normalisasi geometrik digunakan untuk mengubah tekstur iris dalam wilayah annular dari koordinat kartesius ke koordinat pseudo polar melalui model lembaran karet. Proses ini sering disebut sebagai "pembukaan iris" dan menghasilkan entitas persegi panjang yang barisnya sesuai dengan arah sudut pada iris asli dan kolomnya sesuai dengan arah radialnya. Tujuan dari latihan ini ada tiga: (a) memperhitungkan variasi ukuran pupil yang dapat memengaruhi luas spasial iris; (b) karena ukuran pupil dapat bervariasi di seluruh populasi, skema normalisasi memastikan bahwa iris individu yang berbeda dipetakan ke dalam domain gambar umum; dan (c) selama tahap pencocokan, dua iris yang dinormalisasi dapat didaftarkan dengan operasi translasi sederhana yang dapat memperhitungkan kemiringan kepala selama proses akuisisi gambar. Terkait dengan setiap iris yang tidak dibungkus adalah topeng biner yang memberi label piksel iris yang valid dengan "1", sehingga memisahkannya dari piksel yang sesuai dengan kelopak mata dan bulu mata yang diidentifikasi dalam modul segmentasi dan diberi label "0". Normalisasi geometrik diikuti oleh beberapa transformasi fotometrik yang meningkatkan struktur tekstur iris yang tidak dibungkus.
4. **Pengodean dan Pencocokan**: Sementara iris yang tidak dibungkus dapat langsung digunakan untuk membandingkan dua iris (misalnya, dengan menggunakan filter korelasi), biasanya rutinitas ekstraksi fitur digunakan untuk mengodekan konten teksturnya. Sebagian besar algoritme pengodean melakukan analisis multiresolusi iris dengan menerapkan filter wavelet dan memeriksa respons yang dihasilkan. Mekanisme pengodean yang umum digunakan menggunakan Wavelet Gabor 2D kuadratur untuk mengekstrak informasi phasor lokal dari tekstur iris. Setiap respons phasor (besarnya respons tidak digunakan) kemudian dikodekan menggunakan dua bit informasi berdasarkan kuadran bidang kompleks tempatnya berada. Kode biner 2D yang dihasilkan disebut sebagai kode iris. Dua kode iris tersebut dapat dibandingkan menggunakan jarak Hamming, yang menghitung jumlah bit yang sesuai yang berbeda di antara keduanya; topeng biner yang dihitung dalam modul segmentasi digunakan untuk memastikan bahwa hanya bit yang sesuai dengan piksel iris yang valid yang dibandingkan. Sebelum menghitung jarak Hamming, prosedur registrasi mungkin diperlukan untuk menyelaraskan kedua kode iris.

Masing-masing modul ini dijelaskan secara rinci di bagian selanjutnya dari bab ini. Gambar 4.4 memperlihatkan dua aplikasi penting dari sistem pengenalan iris. Aplikasi pertama adalah penggunaan pengenalan iris di bandara untuk mengenali penumpang, karyawan, dan awak pesawat yang membutuhkan akurasi tinggi serta pemrosesan cepat, terutama saat mencocokkan seseorang dengan daftar pantauan. Aplikasi kedua adalah penggunaan pengenalan iris di tambang batu bara. Perlu dicatat bahwa orang-orang yang bekerja di tambang batu bara mungkin tidak dapat memberikan sidik jari atau gambar wajah berkualitas baik karena kondisi kerja.

Gambar 4.4 Contoh praktis sistem pengenalan iris.

(a) Sistem pengenalan iris yang digunakan di UEA untuk mengidentifikasi orang asing yang mencoba masuk kembali ke negara tersebut. (b) Sistem pengenalan iris yang digunakan di tambang batu bara di Cina.

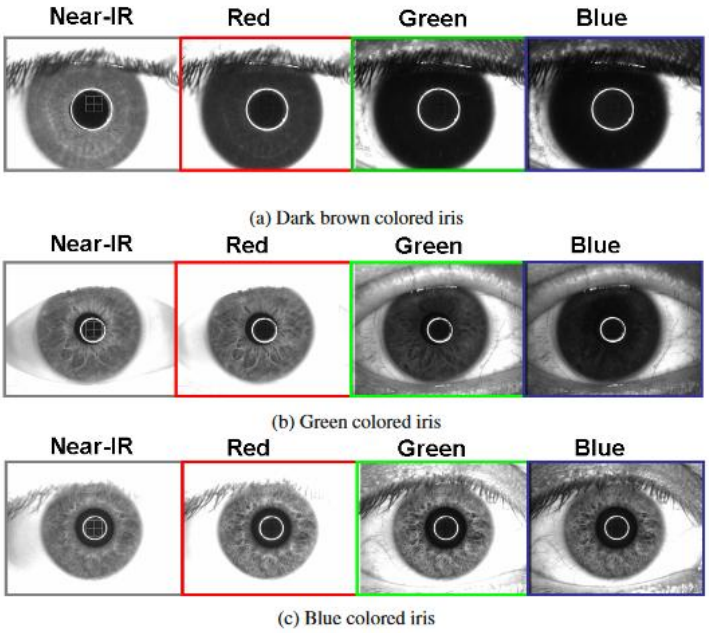
4.3 AKUISISI GAMBAR

Gambar mata diperoleh menggunakan sensor yang peka terhadap spektrum elektromagnetik inframerah dekat (NIR). Ini biasanya sesuai dengan rentang 700nm - 900nm dari pita spektrum inframerah (IR). Penggunaan sensor NIR memiliki setidaknya dua keuntungan yang jelas:

1. Pertama, nuansa tekstur iris berwarna gelap tidak terurai dengan jelas di bagian spektrum elektromagnetik yang tampak2 karena karakteristik penyerapan melanin yang ditemukan di iris. Oleh karena itu, gambar berwarna iris berwarna gelap tidak secara jelas mengungkapkan tekstur iris yang kaya. Meningkatkan panjang gelombang iluminan membantu penetrasi yang lebih baik dari bagian anterior iris berwarna gelap, sehingga mengungkap pola-pola kompleks ini. Oleh karena itu, penggunaan iluminasi NIR bersama dengan sensor NIR lebih disukai untuk memperoleh detail tekstur pada permukaan iris. Hal ini diilustrasikan dalam Gambar 4.5. Tiga baris dalam gambar ini sesuai dengan tiga iris berbeda yang diperoleh menggunakan kamera multispektral. Kamera ini menangkap spektrum merah, hijau, biru, dan NIR dari setiap iris. Baris atas menggambarkan iris cokelat tua, baris tengah menggambarkan iris hijau, dan baris bawah menggambarkan iris biru muda. Seperti yang dapat dilihat dalam gambar ini, detail tekstur iris cokelat tua lebih jelas terlihat di saluran NIR daripada di saluran merah, hijau, atau biru.

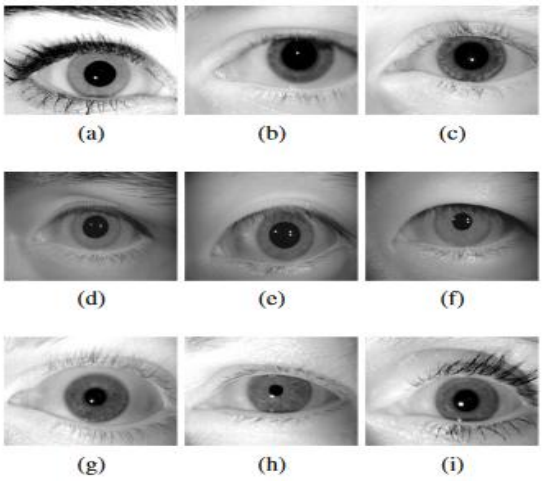
2. Kedua, cahaya NIR tidak dapat dilihat oleh mata manusia. Hal ini memastikan bahwa proses akuisisi gambar tidak mengganggu, bahkan ketika mata harus berada dalam jarak dekat dengan sensor dan sumber cahaya NIR. Biasanya, sumber iluminasi NIR berada di dekat subjek untuk memastikan bahwa daya iluminasi tidak terlalu besar karena dapat membahayakan mata.

Sebagian besar sistem memperoleh serangkaian gambar mata NIR dari subjek dan menggunakan ukuran kualitas untuk memilih subset gambar (sering kali hanya 1 gambar) untuk diproses lebih lanjut. Sebagian besar sistem pengenalan iris membutuhkan 100 - 200 piksel di seluruh iris dalam arah radial untuk pemrosesan yang berhasil. Namun, citra iris dapat terpengaruh secara negatif oleh beberapa faktor, termasuk kelopak mata yang tertutup sebagian, bulu mata yang menonjol, pencahayaan yang kasar atau tidak seragam, resolusi rendah, dan pupil yang sangat melebar atau menyempit. Dengan mengendalikan pencahayaan sekitar secara tepat dan mengharuskan subjek untuk berinteraksi dengan sistem secara kooperatif, beberapa kondisi ini dapat dihindari. Gambar 4.6 menunjukkan contoh citra mata yang diambil dari tiga basis data iris yang tersedia untuk umum.



Gambar. 4.5 Tekstur yang terungkap dalam tiga iris berbeda saat diamati di saluran NIR, merah, hijau, dan biru.

(a) Iris berwarna cokelat tua, (b) iris berwarna hijau, dan (c) iris berwarna biru. Warna iris dinilai secara visual oleh manusia. Perhatikan bahwa pada (a), tekstur iris tidak terdefinisi dengan jelas di saluran merah, hijau, dan biru; namun, terdefinisi lebih baik di saluran NIR. Sebaliknya, pada (c), tekstur iris terdefinisi cukup baik di keempat saluran. Dengan demikian, penggunaan saluran NIR untuk pengenalan iris sangat bermanfaat untuk iris berwarna gelap.



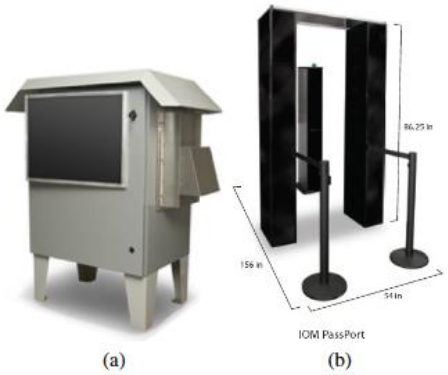
Gambar 4.6 Citra iris dari basis data ICE (baris atas), CASIA versi 3 (baris tengah), dan MBGC (baris bawah). Semua citra ini diperoleh dalam spektrum NIR. Citra ICE dan MBGC diperoleh menggunakan kamera LG EOU 2200, sedangkan citra CASIA versi 3 diperoleh menggunakan perangkat OKI IRISPASS.

Gambar 4.7 mencantumkan beberapa contoh. Panasonic BM-ET 330 adalah perangkat portabel dengan berat sekitar 5 pon dan memiliki jangkauan antara 11,8 dan 15,7 inci. Perangkat ini dapat memperoleh gambar kedua mata secara bersamaan. LG Iris Access 4000 memiliki lensa fokus otomatis dan juga mampu mengambil gambar kedua mata secara bersamaan. Dapat dipasang di dinding dan memiliki jarak operasi antara 10,2 dan 14,2 inci. IRISPASS-M, yang beratnya sekitar 11 pon, juga dapat dipasang di dinding dan memiliki jangkauan operasi antara 1-2 kaki. MobileEyes adalah perangkat penangkap mata ganda yang ditambatkan dengan tangan yang beratnya sekitar 2,8 pon. IGH1000 adalah perangkat iris genggam (namun, dapat juga dipasang di dinding) yang beratnya hanya 750 g. Memiliki jarak fokus antara 4,7 dan 11,8 inci, dan menangkap gambar satu mata.

Pada semua perangkat di atas, mata subjek harus relatif stabil dan berada dalam jarak dekat dengan kamera. Namun, penelitian yang lebih baru telah mengeksplorasi kemungkinan memperoleh pemindaian iris dari subjek yang bergerak yang berada pada jarak yang cukup jauh dari perangkat akuisisi (lihat Gambar 4.8). Ini merupakan tugas yang menakutkan, karena iris adalah objek yang sedikit berosilasi (karena gerakan hippus yang dimulai oleh otot-ototnya) di dalam objek yang bergerak (bola mata), yang terletak di dalam objek bergerak lainnya (kepala)! Lebih jauh, perangkat harus dilengkapi dengan lensa yang memiliki panjang fokus yang panjang (misalnya, 8 inci). Titik choke yang dirancang dengan tepat3 dapat memastikan bahwa pandangan subjek diarahkan ke kamera iris sambil secara bersamaan mengaktifkan iluminan NIR yang ada di sekitar titik choke. Fleksibilitas sistem pengenalan iris saat ini akan ditingkatkan secara substansial jika gambar iris dapat diperoleh dari subjek yang tidak kooperatif dalam lingkungan yang menantang yang ditandai dengan pencahayaan yang keras dan jarak stand-off yang besar.

Gambar 4.7 Contoh perangkat akuisisi citra iris yang dikomersialkan.

(a) Panasonic BM-ET 330, (b) LG IrisAccess 4000, (c) Datastrip Easy Verify, (d) Oki IrisPass, (e) Retica MobileEyes, dan (f) IrisGuard IGH1000. Sebagian besar perangkat akuisisi iris mengharuskan subjek untuk sangat kooperatif dan berada dalam jarak dekat dari kamera. Pencahayaan NIR khusus diperlukan untuk menerangi mata selama akuisisi citra.



Gambar 4.8 Contoh Sistem Iris On The Move (IOM)

(a) Pass Thru, dan (b) Passport Portal. Sistem IOM berpotensi memfasilitasi akuisisi gambar mata secara rahasia untuk pengenalan iris.

4.4 SEGMENTASI IRIS

Kamera iris menangkap gambar mata yang, selain iris, meliputi pupil, kelopak mata, bulu mata, dan sklera. Seperti yang terlihat pada Gambar 4.6, iris dianggap berada di sekitar struktur ini dalam gambar mata 2D. Proses menemukan dan mengisolasi iris dari gambar tersebut dikenal sebagai lokalisasi atau segmentasi iris. Tugas utama segmentasi adalah menentukan piksel dalam gambar yang sesuai dengan wilayah iris.

Segmentasi iris bukanlah tugas yang mudah karena alasan berikut: Tekstur iris menunjukkan tingkat ketidakteraturan yang tinggi dan konten teksturnya sangat bervariasi di antara mata. Memang, iris dapat dilihat sebagai tekstur stokastik yang mengandung banyak fitur seperti "tepi" yang didistribusikan secara acak pada permukaan anteriornya. Model gambar sederhana tidak dapat digunakan untuk mendeskripsikan isinya, sehingga menghalangi penggunaan skema berbasis tampilan (yaitu, skema yang memodelkan tekstur iris berdasarkan tampilan visualnya) untuk pelokalan iris. Iris adalah struktur seperti annular yang dibatasi oleh pupil di perimeter internalnya, dan sklera dan kelopak mata di perimeter eksternalnya. Memperkirakan batas-batas ini (kontur) secara tidak tepat dapat mengakibatkan segmentasi berlebihan atau segmentasi kurang dari entitas iris. Pada beberapa gambar mata, batas-batas ini (terutama batas limbus) mungkin tidak terlalu tajam, sehingga memengaruhi keakuratan proses estimasi batas. Lebih jauh, batas yang ditentukan oleh kelopak mata berbentuk tidak teratur. Tekstur iris mungkin sebagian tertutup oleh bulu mata. Bulu mata yang menonjol ke dalam gambar iris dapat menghasilkan tepi palsu dan memengaruhi proses segmentasi.

Kontras dalam intensitas gambar antara pupil dan iris memberikan petunjuk yang baik untuk mengidentifikasi batas pupil4. Demikian pula, kontras antara iris dan sklera dapat digunakan untuk mendeteksi batas limbus, meskipun besarnya gradien intensitas melintasi batas limbus mungkin lebih kuat daripada batas pupil dalam gambar NIR. Salah satu metode yang paling umum digunakan dalam segmentasi iris bergantung pada deteksi batas-batas ini. Diasumsikan bahwa (a) kedua batas ini dapat didekati menggunakan lingkaran, dan (b) besarnya piksel tepi yang berkontribusi pada batas-batas ini lebih kuat daripada yang berkaitan dengan kontur melingkar lainnya dalam gambar. Seluruh operasi dapat diringkas menggunakan operator integro-diferensial seperti yang dijelaskan di bawah ini.

Segmentasi menggunakan operator integro-diferensial

Operator integro-diferensial, yang dikualifikasi oleh statistik orde (maks), berbentuk

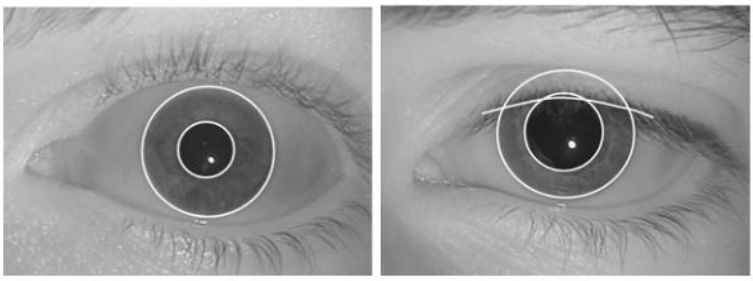
$$max(r,x_0,y_0)\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint_{r,x_0,y_0}\frac{I(x,y)}{2\pi r}ds\right|. \qquad (4.1)$$

Di sini, I adalah citra mata input dan $I(x,y)$ adalah intensitas piksel citra di lokasi (x,y). Menurut Persamaan (4.1), citra I yang diberikan dikonvolusikan dengan filter Gaussian radial $G_\sigma(r)$ dengan skala σ dan radius r. Hal ini penting untuk memastikan bahwa tepi tajam yang sesuai dengan kripta, bintik, dan alur cukup kabur. Selanjutnya, dengan menggunakan lingkaran dengan radius r dan berpusat di (x_0,x_0) pada citra, gradien intensitas piksel-piksel yang terletak pada keliling lingkaran ini dihitung. Untuk setiap piksel, gradien dihitung sepanjang garis yang menghubungkannya ke pusat lingkaran; ini dilambangkan dengan operator diferensial $\frac{\partial}{\partial r}$ .Jumlah nilai gradien ini, sepanjang keliling lingkaran dan dinormalisasi oleh faktor 2πr, kemudian dihitung. Ini dilambangkan dengan operator integral $\oint_{r,X_0Y_0}$dalam Persamaan (4.1). Parameter (r,x_0,y_0) yang menghasilkan

jumlah maksimum diasumsikan untuk menentukan kontur melingkar batas pupil. Prosedur serupa digunakan untuk mendeteksi batas limbus.

Namun, dalam kasus ini, lengkung integrasi dibatasi pada piksel yang hampir vertikal pada keliling lingkaran. Hal ini diperlukan karena kontur limbus dapat disela oleh kelopak mata atas dan bawah dan, oleh karena itu, efek piksel yang tidak termasuk dalam batas limbus harus diminimalkan. Gambar 4.9 mengilustrasikan hasil dari rutinitas segmentasi ini. Pada gambar mata di sebelah kiri, kontur limbus tidak disela oleh kelopak mata. Dengan demikian, daerah annular yang ditentukan oleh kedua batas tersebut hanya berisi piksel yang sesuai dengan iris. Namun, pada gambar mata di sebelah kanan, kontur pupil dan limbus disela oleh kelopak mata. Oleh karena itu, langkah pasca-pemrosesan diperlukan untuk mengidentifikasi batas kelopak mata dan, selanjutnya, mengisolasi piksel-piksel tersebut di dalam daerah annular yang sesuai dengan iris. Perlu dicatat bahwa pusat batas pupil dan limbus biasanya berbeda, yaitu, iris tidak selalu konsentris dengan pupil. Faktanya, pusat pupil berada di bagian nasal (yaitu, bergeser ke arah pangkal hidung) dan lebih rendah dari (yaitu, di bawah) pusat iris.

Kelopak mata dapat dideteksi dengan mencari tepi parabola di dalam daerah yang ditentukan oleh lingkaran luar. Biasanya, prosedur pemasangan spline digunakan untuk mencapai hal ini. Dimungkinkan juga untuk mendeteksi bulu mata yang melanggar tekstur iris dengan mencari tepi yang kuat di dekat vertikal pada iris yang tersegmentasi.



Gambar 4.9 Segmentasi Iris

(a) Citra mata di mana batas pupil dan limbus tidak terputus oleh kelopak mata, dan (b) citra mata di mana kedua batas tersebut diamati terputus oleh kelopak mata. Dalam kasus (b), skema pasca-pemrosesan diperlukan untuk mendeteksi kelopak mata dan mengekstrak piksel iris dari daerah annular yang ditentukan oleh dua kontur melingkar.

Segmentasi menggunakan Kontur Aktif Geodesik (GAC)

Operator integro-diferensial yang dijelaskan di atas (dan variannya) mengasumsikan bahwa batas luar iris dapat diperkirakan menggunakan lingkaran atau elips. Namun, seperti yang disebutkan sebelumnya, keberadaan batas kelopak mata dan bulu mata dalam citra mungkin memerlukan penerapan skema pasca-pemrosesan untuk mendeteksi entitas ini setelah menggunakan operator integro-diferensial. Sebagai alternatif, metode pemasangan kontur tunggal yang secara bersamaan membatasi iris dari sklera serta kelopak mata/bulu mata dapat digunakan. Hal ini dimungkinkan dengan mengadopsi metode kontur aktif yang

dapat mendeteksi batas yang tidak teratur. Dalam subbagian ini, penggunaan Geodesic Active Contours (GAC) untuk mendeteksi batas luar iris akan dijelaskan. Pendekatan ini didasarkan pada hubungan antara kontur aktif dan perhitungan geodesik (kurva panjang minimal). Strateginya adalah mengembangkan kurva yang diinisialisasi secara acak dari dalam iris di bawah pengaruh sifat geometris batas iris. GAC menggabungkan pendekatan minimisasi energi dari "ular" klasik dan kontur aktif geometris berdasarkan evolusi kurva.

Misalkan $\gamma(t)$ adalah kurva yang harus bergerak ke arah batas luar iris pada waktu t tertentu. Waktu t sesuai dengan nomor iterasi. Misalkan ψ adalah fungsi yang mengukur jarak bertanda dari kurva $\gamma(t)$. Yaitu, $\psi\ (x, y)$ = jarak titik (x, y) ke kurva $\gamma(t)$.

$$\psi(x,y) = \begin{cases} 0 & \text{if (x,y) is on the curve;} \\ <0 & \text{if (x,y) is inside the curve;} \\ >0 & \text{if (x,y) is outside the curve.} \end{cases} \tag{4.2}$$

Di sini, ψ berdimensi sama dengan dimensi bayangan mata $I(x, y)$. Kurva $\psi(t)$ disebut himpunan level dari fungsi ψ. Himpunan level adalah himpunan semua titik di ψ di mana ψ adalah suatu konstanta. Jadi ψ = 0 adalah himpunan level ke-nol, ψ = 1 adalah himpunan level pertama, dan seterusnya. ψ adalah representasi implisit dari kurva $\gamma(t)$ dan disebut fungsi penyisipan karena ia menyematkan evolusi $\gamma(t)$. Fungsi penyisipan berevolusi di bawah pengaruh gradien gambar dan karakteristik wilayah sehingga kurva $\gamma(t)$ mendekati batas iris yang diinginkan. Kurva awal $\gamma(t)$ diasumsikan sebagai lingkaran dengan jari-jari r tepat di luar batas pupil. Biarkan kurva $\gamma(t)$ menjadi himpunan level ke-nol dari fungsi penyisipan. Ini menyiratkan bahwa

$$\frac{d\psi}{dt} = 0$$

Dengan aturan rantai,

$$\frac{d\psi}{dt} = \frac{\partial\psi}{\partial x}\frac{dx}{dt} + \frac{\partial\psi}{\partial y}\frac{dy}{dt} + \frac{\partial\psi}{\partial t}$$

Yaitu,

$$\frac{\partial\psi}{\partial t} = -\nabla\psi.\gamma'(t)$$

di mana ∇ adalah operator gradien. Membagi $\gamma(t)$ dalam arah normal $(N(t))$ dan tangensial $(T(t))$,

$$\frac{\partial\psi}{\partial t} = -\nabla\psi.\left(v_N N(t) + v_T T(t)\right)$$

Sekarang, karena ∇ψ tegak lurus terhadap garis singgung ∇ψ,

$$\frac{\partial\psi}{\partial t} = -\nabla\psi.\left(v_N N(t)\right) \tag{4.3}$$

Komponen normal diberikan oleh

$$N = \frac{\nabla \psi}{\|\nabla \psi\|}$$

Substitusikan hal ini ke Persamaan (4.3),

$$\frac{\partial \psi}{\partial t} = -v_N \|\nabla \psi\|$$

Misalkan v_N adalah fungsi kelengkungan kurva κ, fungsi penghentian K (untuk menghentikan evolusi kurva) dan gaya inflasi c (untuk mengembangkan kurva ke arah luar) sehingga,

$$\frac{\partial \psi}{\partial t} = -(div(K\frac{\nabla \psi}{\|\nabla \psi\|}) + cK)\|\nabla \psi\|$$

Dengan demikian, persamaan evolusi untuk ψ_t^5 sehingga γ(t) tetap menjadi himpunan tingkat nol diberikan oleh

$$\psi_t = -K(c + \varepsilon\kappa)\|\nabla \psi\| + \nabla \psi.\nabla K, \tag{4.4}$$

di mana, K, istilah penghentian untuk evolusi, adalah gaya yang bergantung pada gambar dan digunakan untuk memperlambat evolusi di dekat batas; c adalah kecepatan evolusi; ε menunjukkan tingkat kehalusan set level; dan κ adalah kelengkungan set level yang dihitung sebagai

$$\kappa = -\frac{\psi_{xx}\psi_y^2 - 2\psi_x\psi_y\psi_{xy} + \psi_{yy}\psi_x^2}{(\psi_x^2 + \psi_y^2)^{\frac{3}{2}}}$$

Di sini, ψ_x adalah gradien gambar dalam arah x; ψ_y adalah gradien dalam arah y; ψ_{xx} adalah gradien orde ke-2 dalam arah x; ψ_{yy} adalah gradien orde ke-2 dalam arah y; dan ψ_{xy} adalah gradien orde ke-2, pertama dalam arah x dan kemudian dalam arah y. Persamaan (4.4) adalah representasi set level dari model kontur aktif geodesik. Ini berarti bahwa set level C dari ψ berevolusi sesuai dengan

$$C_t = K(c + \varepsilon\kappa)\mathbf{N} - (\nabla K.\mathbf{N})\mathbf{N} \tag{4.5}$$

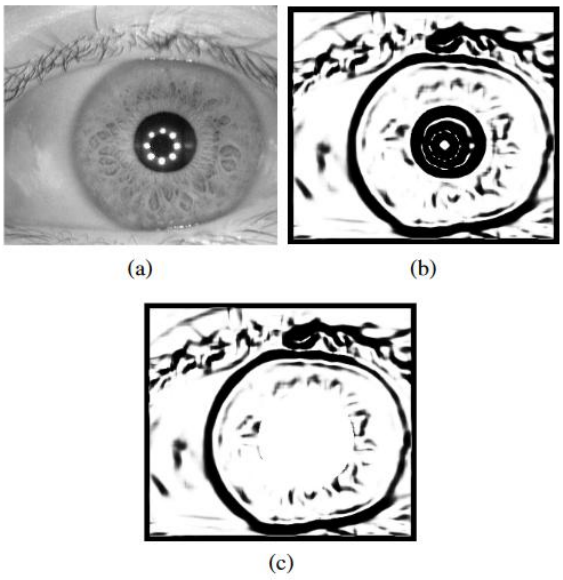
di mana N adalah normal terhadap kurva. Istilah κN memberikan batasan penghalusan pada set level dengan mengurangi kelengkungan totalnya. Istilah cN bertindak

seperti gaya balon dan mendorong kurva ke luar menuju batas objek. Tujuan dari fungsi penghentian adalah untuk memperlambat evolusi saat mencapai batas.

Namun, evolusi kurva akan berakhir hanya saat K = 0, yaitu, di dekat tepi ideal. Pada sebagian besar gambar, nilai gradien akan berbeda di sepanjang tepi, sehingga memerlukan penggunaan nilai K yang berbeda. Untuk menghindari masalah ini, istilah geodesik ketiga ((∇K.N)) diperlukan agar kurva tertarik ke arah batas (∇K menunjuk ke tengah batas). Istilah ini memungkinkan untuk menghentikan proses evolusi bahkan jika (a) fungsi penghentian memiliki nilai yang berbeda di sepanjang tepi, dan (b) celah hadir dalam fungsi penghentian. Istilah penghentian yang digunakan untuk evolusi set level diberikan oleh

$$K(x,y) = \frac{1}{1+\left(\frac{\|\nabla(G(x,y)\star I(x,y))\|}{k}\right)^{\alpha}} \tag{4.6}$$

di mana $I(x,y)$ adalah citra yang akan disegmentasi, $G(x,y)$ adalah filter Gaussian, dan k dan α adalah konstanta. Seperti yang dapat dilihat, $K(x,y)$ bukan fungsi t.



Gambar 4.10 Fungsi Penghentian Untuk Kontur Aktif Geodesik

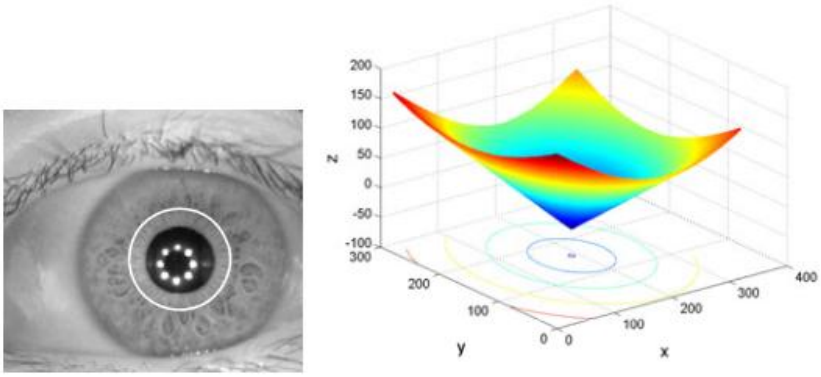
Gambar. 4.10 Fungsi penghentian untuk kontur aktif geodesik. (a) Citra iris asli, (b) fungsi penghentian K, dan (c) fungsi penghentian K' yang dimodifikasi. Pertimbangkan citra iris yang akan disegmentasi seperti yang ditunjukkan pada Gambar 4.10 (a). Fungsi penghentian K yang diperoleh dari citra ini ditunjukkan pada Gambar 4.10 (b) (untuk k = 2,8 dan α = 8). Dengan asumsi bahwa batas iris bagian dalam (yaitu, batas pupil) telah terdeteksi, fungsi penghentian K dimodifikasi dengan menghapus tepi melingkar yang sesuai dengan batas pupil, sehingga menghasilkan fungsi penghentian baru K'. Ini memastikan bahwa set level yang berkembang tidak diakhiri oleh tepi batas pupil (Gambar 4.10 (c)).

Kontur pertama kali diinisialisasi di dekat pupil (Gambar 4.11 (a)). Fungsi penyisipan ψ diinisialisasi sebagai fungsi jarak bertanda ke $\gamma(t = 0)$ yang tampak seperti kerucut (Gambar 4.11 (b)). Diskretisasi persamaan 4.4 menghasilkan persamaan berikut:

$$\frac{\psi_{i,j}^{t+1} - \psi_{i,j}^{t}}{\Delta t} = -cK'_{i,j}\|\nabla\psi^t\| - K'_{i,j}(\varepsilon\kappa_{i,j}^{t}\|\nabla\psi^t\|) + \nabla\psi_{i,j}^{t}.\nabla K_{i,j}^{'t}, \qquad (4.7)$$

di mana Δ t adalah langkah waktu (misalnya, Δ t dapat ditetapkan menjadi 0,05). Suku pertama (cKi', j $\nabla\psi$ t) di sisi kanan persamaan di atas adalah suku kecepatan (suku adveksi) dan, dalam kasus segmentasi iris, bertindak sebagai gaya inflasi. Suku ini dapat menyebabkan singularitas dan karenanya didiskritisasi menggunakan perbedaan hingga yang berlawanan arah angin. Skema berlawanan arah angin untuk memperkirakan $\|\nabla\psi\|$ diberikan oleh

$$\|\nabla\psi\| = \sqrt{A},$$
$$A = min(D_x^- \psi_{i,j}, 0)^2 + max(D_x^+ \psi_{i,j}, 0)^2 +$$
$$min(D_y^- \psi_{i,j}, 0)^2 + min(D_y^+ \psi_{i,j}, 0)^2.$$



(a) (b)

Gambar 4.11 Inisialisasi Kontur Untuk Segmentasi Iris

Gambar 4.11 Inisialisasi kontur untuk segmentasi iris menggunakan GAC. (a) Set level ke nol (kontur awal), (b) plot mesh yang menunjukkan fungsi jarak bertanda ψ. D−x ψ adalah perbedaan mundur orde pertama ψ dalam arah x; D+ ψ adalah perbedaan maju orde pertama dalam arah x; D−y ψ adalah perbedaan mundur orde pertama ψ dalam arah y; dan D+ ψ adalah perbedaan maju orde pertama ψ dalam arah y. Suku kedua (Ki', j ($\nabla\psi$ t j $\nabla\psi$ t)) adalah suku penghalusan berbasis kelengkungan dan dapat didiskritisasi menggunakan perbedaan pusat. Dalam implementasi kami, c = 0,65 dan ε = 1 untuk semua citra iris. Suku geodesik ketiga . ∇ K't) juga didiskritisasi menggunakan perbedaan pusat.

Setelah mengembangkan fungsi penyematan menurut Persamaan (4.7), kurva mulai tumbuh hingga memenuhi kriteria penghentian yang ditetapkan oleh fungsi

penghentian K'. Namun, terkadang, kontur terus berkembang di wilayah lokal gambar tempat kriteria penghentian tidak kuat. Hal ini menyebabkan evolusi kontur yang berlebihan. Hal ini dapat dihindari dengan meminimalkan energi spline pelat tipis dari kontur. Dengan menghitung perbedaan energi antara dua kontur yang berurutan, skema evolusi dapat diatur. Jika perbedaan antara kontur kurang dari ambang batas (yang menunjukkan bahwa evolusi kontur telah berhenti di sebagian besar tempat), maka proses evolusi kontur dihentikan.

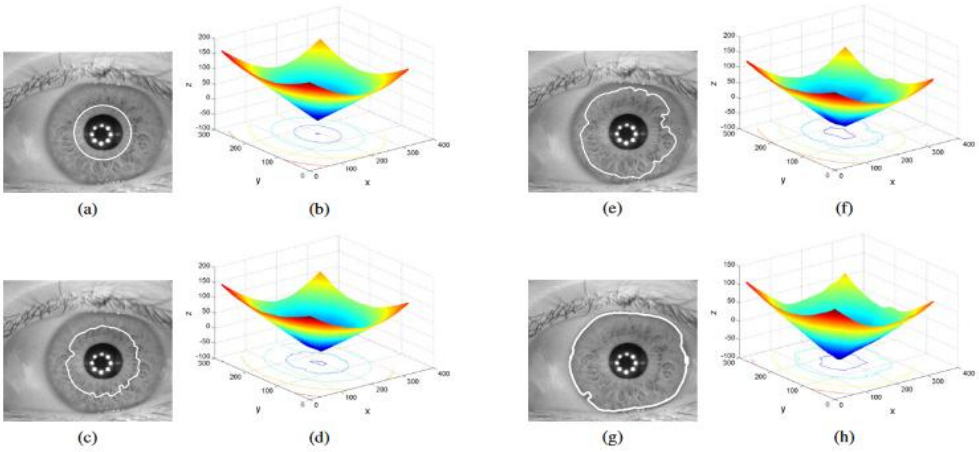
Evolusi kurva dan fungsi penyematan yang sesuai diilustrasikan dalam Gambar 4.12. Karena serat radial mungkin tebal di bagian tertentu iris, atau kripta yang ada di wilayah silia mungkin sangat gelap, hal ini dapat menyebabkan tepi yang menonjol dalam fungsi penghentian. Jika teknik segmentasi didasarkan pada kurva parametrik, maka evolusi kurva mungkin berakhir pada titik minimum lokal ini. Namun, kontur aktif geodesik dapat terbelah pada titik minimum lokal tersebut dan bergabung lagi. Dengan demikian, kontur aktif geodesik dapat secara efektif menangani masalah titik minimum lokal, sehingga memastikan bahwa kontur akhir sesuai dengan batas limbus yang sebenarnya (Gambar 4.13).

Pembuatan masker iris

Iris yang terlokalisasi berpotensi tersumbat karena area bising lainnya seperti bulu mata, bayangan, atau pantulan spekular. Dengan demikian, masker bising dihasilkan, yang merekam lokasi penyumbatan iris yang tidak diinginkan tersebut.

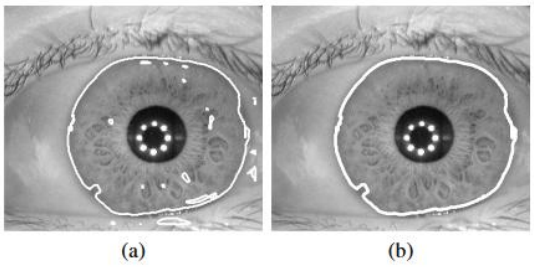
4.5 NORMALISASI IRIS

Jumlah tekstur iris (yaitu, luas spasialnya) yang terungkap dalam gambar dapat dipengaruhi oleh sejumlah faktor. Yang terpenting di antaranya adalah pelebaran dan kontraksi pupil sebagai respons terhadap pencahayaan sekitar. Ukuran iris (yaitu, jumlah piksel iris yang valid) meningkat saat pupil berkontraksi sebagai respons terhadap cahaya terang dan berkurang saat pupil melebar dalam cahaya redup. Selain itu, faktor-faktor seperti resolusi sensor dan jarak pencitraan juga memengaruhi jumlah piksel iris yang dapat diperoleh dari gambar mata. Lebih jauh, ukuran pupil dapat bervariasi antar individu. Untuk mengatasi variasi ukuran ini, iris yang tersegmentasi dibuka dan diubah dari koordinat kartesius ke sistem koordinat pseudo-polar yang dinormalkan. Operasi normalisasi ini dilakukan dengan merepresentasikan iris yang tersegmentasi sebagai gambar persegi panjang, yang baris-barisnya sesuai dengan daerah konsentris iris. Transformasi ini disebut model lembaran karet Daugman dan memetakan ulang setiap titik di daerah annular antara dua batas melingkar (yaitu, batas pupil dan limbus) ke koordinat pseudo-polar (r, θ), di mana r ∈ [0,1] dan $\theta \in [0,2\pi]$, seperti yang ditunjukkan pada Gambar 4.14.



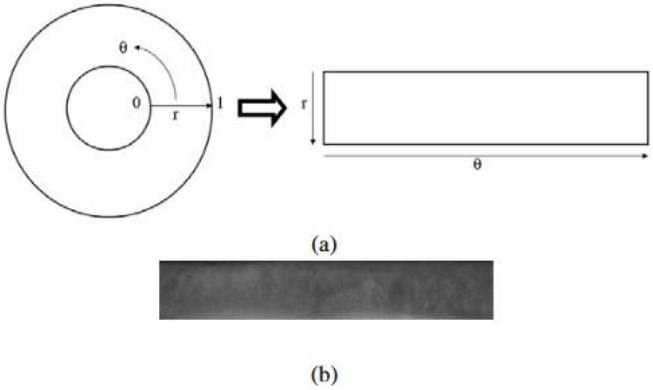
Gambar 4.12 Evolusi Kontur Aktif Geodesic Selama Segmentasi Iris

Gambar 4.12 Evolusi kontur aktif geodesik selama segmentasi iris. (a) Citra iris dengan kontur awal, (b) fungsi penyematan □ (sumbu X dan Y sesuai dengan luas spasial citra mata dan sumbu Z mewakili set level yang berbeda), (c,d,e,f) kontur setelah 600 dan 1400 iterasi, dan fungsi penyematan yang sesuai, dan (g,h) Kontur akhir setelah 1800 iterasi (kontur ditunjukkan dengan warna putih).



Gambar 4.13 Kontur Akhir Iris

Gambar 4.13 Kontur akhir yang diperoleh saat melakukan segmentasi iris menggunakan skema GAC. (a) Contoh pemisahan kontur geodesik pada berbagai titik minimum lokal, (b) kontur akhir (kontur ditunjukkan dengan warna putih).



Gambar 4.14 Normalisasi iris.

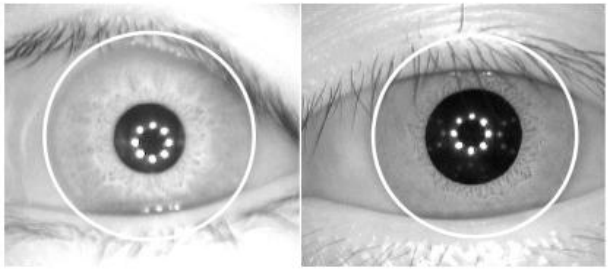
(a) Model lembaran karet Daugman digunakan untuk normalisasi iris. Rutin normalisasi mengubah koordinat piksel di daerah annular antara batas pupil dan limbus menjadi koordinat polar. Ini mengatasi masalah variasi ukuran pupil di beberapa gambar. (b) Contoh iris yang dinormalisasi. Pemetaan ulang daerah iris I dari koordinat kartesius (x, y) ke koordinat polar yang dinormalisasi (r, θ) dinyatakan sebagai:

$$I(x(r,\theta),y(r,\theta)) \rightarrow I(r,\theta), \tag{4.8}$$

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta), \tag{4.9}$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta), \tag{4.10}$$

di mana x_p, y_p dan x_l, y_l adalah koordinat titik yang diambil sampelnya dari batas pupil dan limbus, masing-masing. Bersamaan dengan iris yang terlokalisasi, topeng derau juga dibuka untuk memfasilitasi pencocokan yang lebih cepat. Untuk memperhitungkan ketidakteraturan dan efek kelopak mata/bulu mata pada batas limbus yang diekstraksi menggunakan skema GAC, hanya titik-titik pada kontur yang terletak pada batas iris dan sklera (berlawanan dengan batas iris dan kelopak mata) yang digunakan untuk memperkirakan radius dan pusat iris. Secara khusus, enam titik pada sudut [300, 00, 300, 1500, 1800, 2100] terhadap sumbu horizontal dipilih dari kontur yang diekstraksi dan jarak rata-ratanya dari pusat pupil digunakan sebagai perkiraan radius iris (R). Sebuah lingkaran selanjutnya dipasang melalui semua titik pada kontur yang berada dalam jarak R piksel dari pusat pupil. Lingkaran ini memperkirakan batas limbus iris yang sebenarnya. Gambar 4.15 menunjukkan prosedur ini.



(a) (b)

Gambar. 4.15 Ketika GAC digunakan untuk melokalisasi batas iris luar, maka langkah tambahan diperlukan untuk memfasilitasi normalisasi.

Dengan demikian, batas tak beraturan yang disimpulkan menggunakan kontur aktif diubah menjadi batas melingkar seperti yang ditunjukkan pada gambar di atas. Piksel-piksel yang termasuk dalam batas melingkar, tetapi dikecualikan oleh batas tak beraturan dianggap sebagai piksel non-iris dan dikecualikan oleh topeng.

4.6 PENGODEAN DAN PENCOCOKAN IRIS

Proses mengekstraksi kumpulan fitur numerik dari iris disebut pengodean iris. Ini sesuai dengan tahap ekstraksi fitur yang ditunjukkan dalam Bab 1. Untuk mengodekan pola tekstur iris yang dinormalisasi, wavelet Gabor dua dimensi biasanya dikonvolusi dengan gambar iris yang tidak dibungkus. Wavelet Gabor 2D, di atas domain gambar (x, y), diberikan oleh:

$$G(x,y) = e^{-\pi[(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]}e^{-2\pi i[(u_0(x-x_0)+v_0(y-y_0)]}, \qquad (4.11)$$

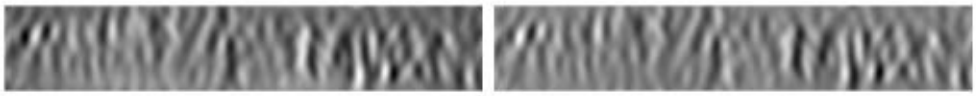
di mana (x_0, y_0) menyatakan posisi dalam gambar, (α, β) menyatakan lebar dan panjang efektif, dan (u_0, v_0) memastikan arah gelombang dengan frekuensi spasial $\omega_0 = \sqrt{u_0^2 + v_0^2}$ Komponen nyata dan imajiner dari wavelet ini dapat dipisahkan sebagai berikut:

$$\Re\{G(x,y)\} = e^{-\pi[(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]}\cos(-2\pi[(u_0(x-x_0)+v_0(y-y_0)]), \qquad (4.12)$$

Dan

$$\Im\{G(x,y)\} = e^{-\pi[(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]}\sin(-2\pi[(u_0(x-x_0)+v_0(y-y_0)]), \qquad (4.13)$$

Output riil dan imajiner yang diperoleh dengan menggabungkan wavelet Gabor 2D dengan citra iris yang dinormalisasi ditunjukkan pada Gambar 4.16



(a) (b)

Gambar 4.16 Output riil dan imajiner dari penggabungan gambar dengan wavelet Gabor 2D.

Output wavelet Gabor didemodulasi untuk mengompresi data. Hal ini dilakukan dengan mengkuantisasi informasi fase menjadi empat level yang berbeda, satu untuk setiap kuadran bidang kompleks. Karena normalisasi dilakukan sebelumnya dalam koordinat kutub, wavelet dalam koordinat kutub dapat dinyatakan sebagai:

$$H(r,\theta) = e^{-i\omega(\theta-\theta_0)}e^{-(r-r_0)^2/\alpha^2}e^{-i(\theta-\theta_0)^2/\beta^2}, \qquad (4.14)$$

di mana (r_0, θ_0) menunjukkan frekuensi pusat wavelet, sementara semua variabel lainnya menunjukkan parameter yang sama seperti pada Persamaan (4.11). Dengan citra iris

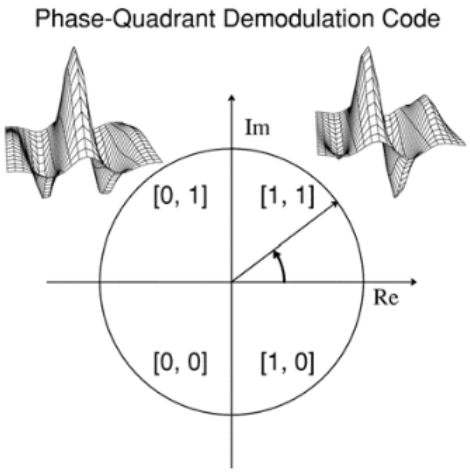
ternormalisasi I(ρ, ϕ) dalam sistem koordinat polar, proses demodulasi dan kuantisasi fase dapat ditulis sebagai:

$$h_{Re,Im} = sign_{Re,Im} \int_{\rho} \int_{\phi} I(\rho, \phi) e^{-i\omega(\theta_0 - \phi)} e^{-(r_0 - \rho)^2/\alpha^2} e^{-(\theta_0 - \phi)^2/\beta^2} \rho d\rho d\phi, \quad (4.15)$$

di mana $h_{Re,Im}$ adalah bit bernilai kompleks yang komponen riil dan imajinernya bergantung pada tanda integral. Hal ini diilustrasikan dalam Gambar 4.17. Respons dari operasi ini adalah keluaran biner yang disebut kode iris. Dimensi (atau panjang) kode iris bergantung pada ukuran citra iris yang dinormalkan, yang pada gilirannya bergantung pada resolusi sepanjang sumbu r dan θ. Dimensi 2048 umumnya digunakan. Jarak Hamming (HD) yang dinormalkan antara dua kode iris digunakan sebagai ukuran ketidaksamaan antara dua iris. Nilai ini dihitung dengan menutupi setiap kode iris dengan topengnya masing-masing untuk mengabaikan daerah yang bising. Jarak Hamming antara dua kode iris dihitung sebagai

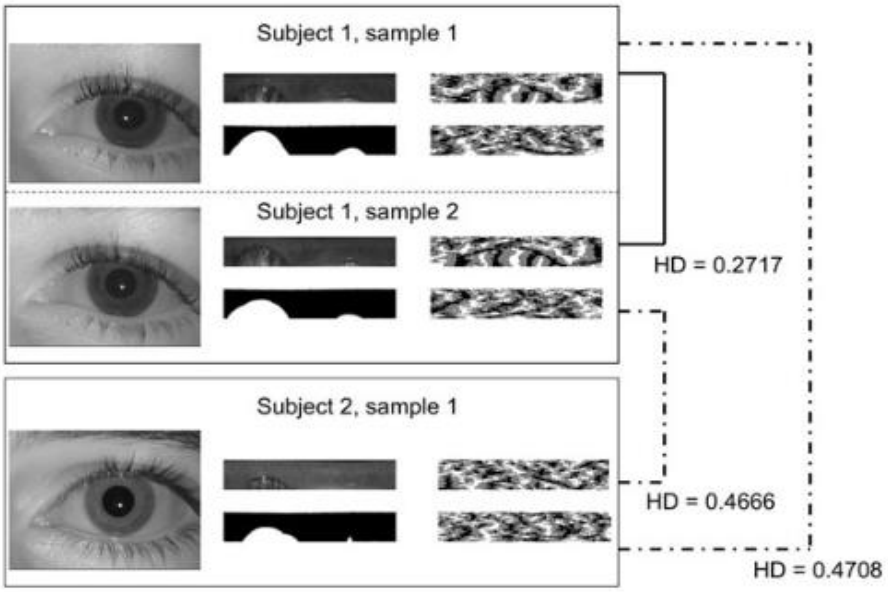
$$HD = \frac{\| (IrisKodeA \oplus IrisKodeB) \cap MaskA \cap MaskB \|}{\| MaskA \cap MaskB \|} \quad (4.16)$$

Operator XOR ($\oplus$) mendeteksi bit yang tidak sama antara dua kode iris, sedangkan operator AND ($\cap$) menutupi daerah yang tidak selaras. Penyebut membantu dalam menormalkan jumlah total bit yang tidak sama dalam interval [0, 1]. Kecocokan sempurna antara dua kode iris akan menghasilkan nilai HD sebesar 0. Lihat Gambar 4.18.



Gambar 4.17 Ilustrasi proses demodulasi dan kuantisasi fase yang digunakan untuk mengodekan iris.

Respons fasor pada setiap piksel dalam iris yang dinormalisasi dikuantisasi menjadi dua bit informasi.

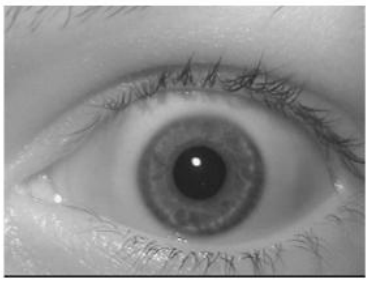


Gambar. 4.18 Proses pencocokan sepasang iris.

Di sini, tiga gambar mata milik dua subjek berbeda ditampilkan. Setiap gambar dikenakan rutinitas segmentasi untuk mengekstrak iris, yang diubah menjadi entitas persegi panjang melalui model lembaran karet Daugman. Rutin segmentasi menghasilkan topeng biner, di mana 1 menunjukkan piksel iris dan 0 menunjukkan piksel non-iris. Iris yang dinormalisasi diproses menggunakan wavelet Gabor dan respons phasor yang dihasilkan dikuantisasi menjadi kode iris. Jarak Hamming (HD) antara dua kode iris dari iris yang sama diharapkan lebih kecil daripada yang sesuai dengan dua iris yang berbeda.

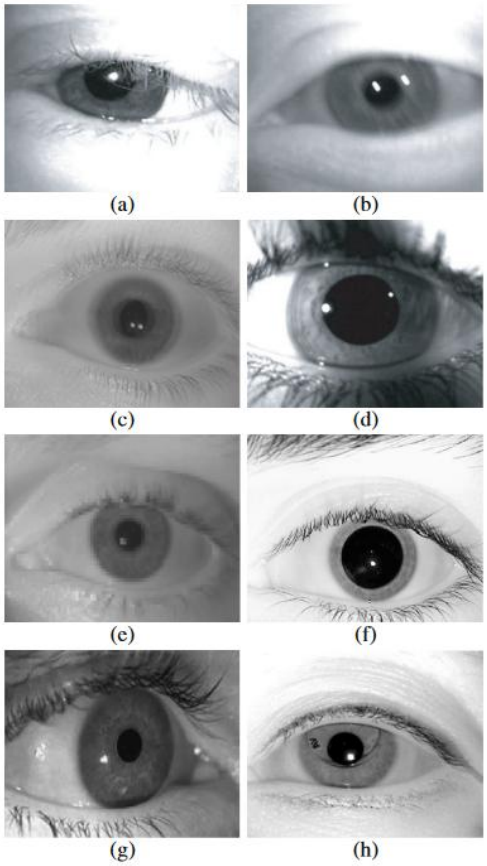
4.7 KUALITAS IRIS

Tergantung pada bidang pandang sensor iris, citra iris biasanya mencakup bulu mata atas dan bawah serta kelopak mata, dan beberapa area alis seperti yang ditunjukkan pada Gambar 4.19. Namun, hanya informasi tekstur iris yang kaya antara batas pupil dan limbus yang digunakan untuk pengenalan. Jadi, untuk citra iris tertentu (atau bingkai video), evaluasi kualitas biasanya didasarkan pada faktor-faktor yang menurunkan atau mengurangi ukuran area iris.



Gambar 4.19 Contoh gambar iris NIR yang diambil dari pengguna kooperatif dalam kondisi yang hampir ideal.

Beberapa faktor yang dapat secara signifikan mengurangi kualitas gambar iris meliputi (a) oklusi, (b) defokus, atau tidak fokus, (c) gerakan kabur, (d) iluminasi tidak seragam, (e) resolusi rendah, atau jarak pencitraan besar, (f) dilatasi iris, (g) pencitraan miring, dan (h) keberadaan aksesori seperti lensa kontak palsu atau cetak. Contoh-contoh ditunjukkan pada Gambar 4.20.



Gambar 4.20 Kualitas gambar iris yang buruk disebabkan oleh (a) oklusi, (b) defokus, (c) kaburnya gerakan, (d) iluminasi yang tidak seragam, (e) sensor resolusi rendah, (f) dilatasi iris, (g) pencitraan sudut miring, dan (h) keberadaan lensa kontak tercetak.

Teknik Penilaian Kualitas

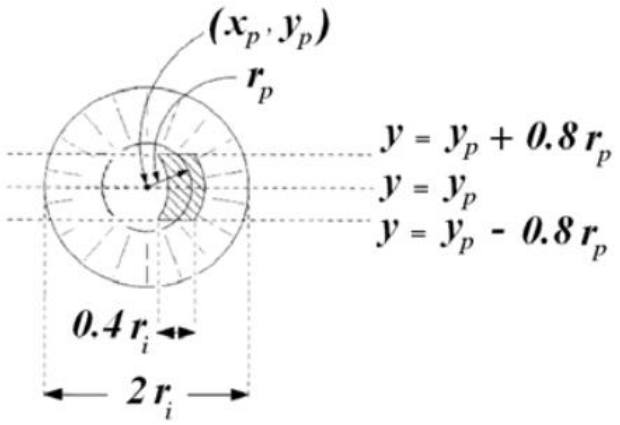
Sementara sebagian besar skema evaluasi kualitas hanya mempertimbangkan satu atau sepasang faktor, teknik yang lebih baru mempertimbangkan berbagai faktor yang lebih luas untuk penilaian kualitas. Beberapa di antaranya dijelaskan di sini , Menguji ketajaman bagian antara pupil dan iris: Ketajaman gambar biasanya merupakan indikator pemfokusan yang tepat dari objek yang sedang dicitrakan dan dengan demikian biasanya digunakan dalam menentukan kualitas gambar iris. Di sini, ketajaman pada dasarnya dihitung sebagai besaran normal dari gradien intensitas di dekat batas pupil. Misalkan (Xp,Yp) dan rp masing-masing menunjukkan pusat dan jari-jari pupil, dan ri menunjukkan jari-jari iris. Suatu wilayah minat dipilih sedemikian rupa sehingga semua piksel (x, y) yang terletak di dalam wilayah tersebut memenuhi kondisi berikut:

$$(y_p - 0.8r_p) < y < (y_p + 0.8r_p) \tag{4.17}$$

Dan

$$-\sqrt{r_p^2 - (y-y_p)^2} + 0.1r_i < x - x_p < -\sqrt{r_p^2 - (y-y_p)^2} + 0.2r_i \tag{4.18}$$

Gambar 4.21 mengilustrasikan wilayah minat yang ditentukan oleh kondisi di atas.



Gambar 4.21 Wilayah minat yang dipilih untuk memperkirakan ketajaman iris.

Dari wilayah minat yang dipilih, nilai median piksel yang berada di wilayah pupil, M_p, dan wilayah iris, M_i, dihitung. Kemudian, untuk semua piksel di wilayah yang dipilih yang nilai intensitasnya berada di antara M_p dan M_i, nilai absolut gradien horizontalnya dikumpulkan dalam satu set. Dari set ini, rata-rata dari 20 nilai teratas dihitung, dan dilambangkan dengan variabel S. Ukuran ketajaman gambar iris tertentu, $\frac{1}{w}$, kemudian dihitung dengan persamaan berikut:

$$\frac{1}{w} = \frac{S}{H}, \tag{4.19}$$

di mana $H = (M_i - M_p)$ menunjukkan ukuran langkah. Jika ukuran ketajaman berada di atas nilai ambang 0,5, gambar dianggap terfokus dengan baik dan, oleh karena itu, berkualitas baik. Mengukur energi frekuensi spasial tinggi di seluruh gambar: Metode ini menentukan ketajaman di seluruh gambar menggunakan analisis Fourier 2D untuk menghilangkan gambar yang tidak fokus secara optik. Untuk gambar tertentu yang direpresentasikan sebagai fungsi 2D bidang nyata $I(x, y)$, transformasi Fourier 2D-nya F (μ, ν) didefinisikan oleh:

$$F(\mu,\nu) = \frac{1}{(2\pi)^2} \int\int I(x,y) \exp(-i(\mu x + \nu y)) dx dy. \tag{4.20}$$

Gambar yang tidak fokus, D$\sigma(\mu, \nu)$, terkait dengan transformasi Fourier 2D dari gambar fokus yang sesuai, F(μ, ν), dengan model berikut:

$$D_\sigma(\mu,\nu) = \exp\left(-\frac{\mu^2+\nu^2}{\sigma^2}\right)F(\mu,\nu). \quad (4.21)$$

Pengaburan terutama melemahkan frekuensi tertinggi dalam gambar, sementara komponen frekuensi rendah hampir tidak terpengaruh. Hal ini karena suku eksponensial dalam persamaan di atas mendekati satu ketika frekuensi (μ,ν) menjadi kecil. Dengan demikian, metode yang efektif untuk mengidentifikasi gambar yang tidak fokus adalah dengan mengukur daya totalnya dalam domain Fourier 2D pada frekuensi spasial yang lebih tinggi (karena daya tersebut paling dilemahkan oleh pengaburan). Untuk membuat pengukuran kualitas ini independen dari konten gambar, rasio daya pita frekuensi yang lebih tinggi dapat dibandingkan dengan pita frekuensi yang lebih rendah.

Menganalisis spektrum Fourier dari daerah iris lokal: Hal ini dapat digunakan untuk mendeteksi gambar berkualitas buruk yang disebabkan oleh faktor-faktor seperti (a) keburaman yang tidak fokus, (b) keburaman gerakan, dan (c) oklusi karena bulu mata, dan/atau kelopak mata. Analisis Fourier dari gambar iris tertentu menghasilkan sejumlah besar informasi, yang dapat digunakan untuk mengisolasi gambar berkualitas buruk dari sekumpulan gambar tertentu. Untuk gambar yang tidak fokus, spektrum Fourier seharusnya sebagian besar didominasi oleh komponen frekuensi rendah. Di sisi lain, gambar iris dengan oklusi mengandung komponen frekuensi menengah dan tinggi yang signifikan yang disebabkan oleh bulu mata. Spektrum Fourier dari gambar yang kabur karena gerakan tidak memiliki komponen frekuensi menengah dan tinggi, dan memiliki distribusi frekuensi yang mirip dengan gambar yang tidak fokus.

Deskriptor yang digunakan untuk memperkirakan kualitas gambar iris kemudian dapat didefinisikan sebagai:

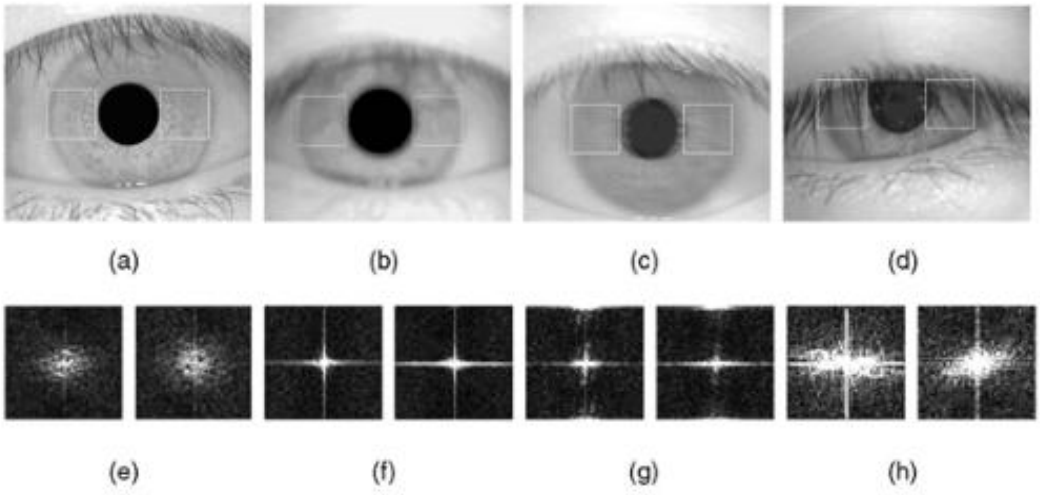
$$D = \left[(F_1 + F_2 + F_3); \frac{F_2}{F_1 + F_3}\right], \quad (4.22)$$

Dimana

$$F_i = \int\int_{\Omega = \{(u,v)|f_1^i < \sqrt{u^2+v^2} <= f_2^i\}} |F(u,v)|\, dudv \quad i = 1,2,3, \quad (4.23)$$

dan $F(u,v)$ adalah spektrum Fourier 2D dari daerah iris, sementara F_1, F_2 dan F_3 masing-masing menunjukkan daya komponen frekuensi rendah, menengah, dan tinggi. Frekuensi f_1^i dan f_2^i adalah pasangan frekuensi radial, yang membentuk ekstrema dari komponen frekuensi yang sesuai. Deskriptor kualitas D terdiri dari dua fitur frekuensi pembeda. Fitur pertama adalah daya spektrum total daerah iris yang secara efektif dapat membedakan gambar iris yang sangat tertutup dari gambar berkualitas tinggi. Fitur kedua adalah rasio daya frekuensi menengah terhadap daya frekuensi lainnya. Untuk gambar yang difokuskan dengan jelas, rasio ini tinggi, jika dibandingkan dengan gambar yang tidak fokus atau kabur karena gerakan. Untuk gambar iris tertentu, I, dua daerah 64x64 dipilih seperti yang ditunjukkan pada Gambar 4.22, dan nilai deskriptor kualitas dihitung. Rata-rata dari dua deskriptor kualitas lokal yang dihasilkan dianggap sebagai ukuran kualitas yang tepat

dari gambar iris. Mengukur energi dari wavelet 2D pada pita konsentris lokal iris: Pendekatan ini mengevaluasi kualitas gambar iris tertentu menggunakan wavelet 2D pada pita konsentris lokal iris yang tersegmentasi. Ukuran kualitas lokal kemudian digunakan sebagai skema pembobotan dalam proses pencocokan untuk menghasilkan hasil yang lebih baik. Analisis dilakukan pada daerah lokal karena kualitasnya dapat bervariasi dari satu daerah ke daerah lainnya. Dengan demikian, metode ini menggunakan bobot yang lebih tinggi untuk daerah bagian dalam iris yang lebih stabil dibandingkan dengan daerah bagian luar yang lebih rentan terhadap oklusi.



Gambar 4.22 (a) Citra iris dengan kualitas baik.

Citra iris dengan kualitas buruk, disebabkan oleh (b) tidak fokus, (c) gerakan kabur, dan (d) oklusi. Citra (e), (f), (g), dan (h) menunjukkan spektrum Fourier dari dua daerah iris lokal yang dipilih berukuran 64 × 64 (disorot oleh kotak putih), yang masing-masing sesuai dengan citra (a), (b), (c), dan (d). Citra direproduksi dari [23]. ⓒ IEEE.

Diberikan sebuah gambar $I(x, y) \in R^2$, Transformasi Wavelet Kontinu (Continuous Wavelet Transform/CWT), yang didefinisikan sebagai konvolusi dengan serangkaian fungsi wavelet, diberikan oleh persamaan berikut:

$$w(s, x_0, y_0) = \frac{1}{\sqrt{s}} \int \int_{R^2} I(x,y) \phi \left(\frac{x - x_0}{s}, \frac{y - y_0}{s} \right) dxdy, \qquad (4.24)$$

di mana s adalah faktor dilatasi (skala), dan (a, b) menunjukkan faktor translasi (pergeseran). Wavelet ϕ dianggap sebagai wavelet topi Meksiko, yang pada dasarnya adalah filter band pass untuk deteksi tepi pada skala s. Pilihan wavelet ini karena sensitivitasnya yang tinggi terhadap fitur yang menunjukkan variasi tajam (misalnya, lubang, bintik, dll.) dan non-linearitas (misalnya, kerah, alur, dll.). Pertama, untuk menangkap berbagai fitur pada beberapa skala, respons produk diperoleh, yang diberikan oleh persamaan berikut:

$$w^{mul}(s_1, s_2, s_3) = w(s_1) \times w(s_2) \times w(s_3). \quad (4.25)$$

Di sini, s_1, s_2, s_3 adalah tiga skala yang dipertimbangkan. Untuk melakukan evaluasi kualitas citra iris, iris disegmentasi untuk memperoleh batas pupil dan iris. Iris yang disegmentasi kemudian dibagi menjadi beberapa pita konsentris dengan lebar tetap, yang berpusat di pusat pupil.

Untuk memperoleh ukuran kualitas lokal, energi E_t dari pita ke-t ($t = 1, 2, \ldots T$), di mana T menunjukkan jumlah total pita, dihitung dengan persamaan berikut:

$$E_t = \frac{1}{N_t} \sum_{i=1}^{i=N_t} | w_{t,i}^{mul} |^2, \quad (4.26)$$

di mana $w_{t,i}^{mul}$ merupakan representasi koefisien wavelet berbasis produk ke-i pada pita ke-t, dan N_t merupakan jumlah total koefisien wavelet pada pita ke-t. Energi, E_t, dianggap sebagai indikator yang baik untuk kekhasan fitur iris, dan karenanya merupakan ukuran kualitas lokal yang dapat diandalkan. Nilai E_t yang tinggi menunjukkan citra berkualitas baik.

Indeks kualitas seluruh citra iris, Q, didefinisikan sebagai rata-rata tertimbang dari nilai kualitas lokal per pita, dan diberikan oleh:

$$Q = \frac{1}{T} \sum_{t=1}^{T} (m_t \times \log(E_t)), \quad (4.27)$$

di mana T menunjukkan jumlah total pita dan mt adalah bobot, diberikan oleh $m_t = \exp\{-\|l_t - l_c\|^2/(2q)\}$. Variabel l_c menunjukkan pusat pupil, dan l_t menunjukkan jari-jari rata-rata pita ke-t terhadap l_c.

Untuk memasukkan ukuran kualitas lokal ke dalam skema pencocokan, algoritma pencocokan jarak Hamming Daugman dimodifikasi sebagai:

$$HD_w = \frac{1}{B} \frac{\sum_{i=1}^{B} \sqrt{E_{g(i)}^X \times E_{g(i)}^Y} \times (X_i \otimes Y_i)}{\sum_{i=1}^{B} \sqrt{E_{g(i)}^X \times E_{g(i)}^Y}}, \quad (4.28)$$

di mana X_i dan Y_i masing-masing mewakili bit ke-i dari urutan kode iris X dan Y, dan N adalah jumlah total bit dalam urutan tersebut. g(i) adalah indeks pita yang berisi bit ke-i dari IrisCode, dan $E_{\mathrm{g(i)}}^X dan\, E_{g(i)}^Y$ adalah ukuran kualitas lokal pita ke-$g(i)$ di X dan Y, masing-masing. Simbol tersebut mewakili operasi logika XOR.

Penilaian kualitas citra iris merupakan area penelitian yang terus berlanjut. Meskipun penelitian awal telah menunjukkan manfaat dari penggabungan kualitas iris, penilaian dan penggunaannya dalam lingkungan waktu nyata masih merupakan tantangan terbuka.

4.8 EVALUASI KINERJA

Menurut literatur biometrik, tekstur struktural pada iris sangat beragam di seluruh populasi. Seperti yang dinyatakan sebelumnya, bahkan iris pada kembar monozigot menunjukkan perbedaan struktural. Pengujian skala besar telah mengonfirmasi potensi pola iris untuk mengidentifikasi individu dalam basis data subjek yang besar. Eksperimen yang dilakukan oleh Daugman pada basis data berisi 632.500 gambar iris (316.250 orang yang mencakup 152 negara) menunjukkan kemungkinan kebijakan keputusan yang dapat menghasilkan tingkat kesalahan nol. Namun, tingkat ini didasarkan pada kualitas gambar iris, yang harus dipantau secara ketat untuk memastikan kejelasan tekstur yang wajar. Pengujian yang dilakukan pada tahun 2006 oleh Institut Nasional Standar dan Teknologi yang melibatkan berbagai kualitas gambar menunjukkan bahwa tingkat ketidakcocokan palsu dari algoritma pengenalan iris dengan kinerja terbaik dapat bervariasi antara 1,1 hingga 1,4 persen pada tingkat kecocokan palsu sebesar 0,1 persen.

RINGKASAN

Kemajuan luar biasa dalam sistem pengenalan iris telah menghasilkan beberapa tantangan dan peluang baru, yang telah menjadi fokus upaya penelitian terkini. Kami menyimpulkan bab ini dengan mencantumkan beberapa tantangan tersebut.

Iris adalah objek bergerak dengan luas permukaan kecil, yang berada di dalam bola mata yang dapat bergerak secara independen dari iris. Bola mata pada gilirannya berada di dalam kepala, objek bergerak lainnya. Oleh karena itu, tantangan beratnya adalah menemukan bola mata dengan andal dan melokalisasi posisi iris dalam gambar yang diperoleh dari jarak jauh dari subjek manusia yang tidak dibatasi. Karena modul akuisisi biasanya mencitrakan iris dalam spektrum NIR, diperlukan pencahayaan tak kasat mata yang tepat untuk menerangi iris saat memperoleh gambar. Faktor-faktor ini membingungkan kemampuan sistem untuk beroperasi dengan sukses saat subjek berada lebih dari beberapa meter dari kamera. Upaya terkini telah berhasil merancang dan mengembangkan sistem pengenalan iris saat bergerak dan iris pada jarak jauh. Upaya lain adalah menyelidiki teknologi seperti pencitraan berkode muka gelombang untuk meningkatkan kedalaman bidang kamera.

Iride yang tidak ideal dapat disebabkan oleh gerakan kabur, difusi kamera, gangguan transmisi, pencitraan yang tidak fokus, oklusi dari kelopak mata dan bulu mata, rotasi kepala, pandangan yang tidak sejajar dengan sumbu atau sudut kamera, pantulan spekular, kontras yang buruk, dan luminositas alami - faktor-faktor yang dapat menyebabkan rasio ketidakcocokan palsu yang lebih tinggi. Skema pemulihan citra yang kuat diperlukan untuk meningkatkan kualitas citra iris tersebut sebelum sistem memprosesnya. Penelitian terkini telah berupaya menangani masalah citra iris yang tidak sejajar dengan sumbu dengan merancang model kalibrasi dan koreksi geometrik yang sesuai.

Asumsi umum adalah bahwa relief tekstur iris bersifat unik karena morfogenesisnya yang acak, dan evaluasi empiris skala besar telah mengonfirmasi gagasan ini di sebagian besar populasi. Namun, tidak ada model teoritis yang efektif untuk mengukur individualitas

iris. Meskipun para peneliti telah menggunakan distribusi skor kecocokan dan statistik IrisCode untuk menyimpulkan derajat kebebasan biometrik iris, belum ada yang secara langsung menggunakan dasar biologis iris untuk memastikan individualitasnya. Masalah menarik ini memiliki implikasi untuk menggunakan pengenalan iris di pengadilan sesuai dengan kriteria penerimaan Daubert dan Aturan Pembuktian Federal.

Dengan menggabungkan iris dengan fitur mata lainnya seperti pembuluh darah konjungtiva, para peneliti mungkin dapat mengembangkan sistem multibiometrik berbasis mata yang kuat yang dapat beroperasi di lingkungan yang dicirikan oleh pencahayaan yang keras, subjek yang bergerak, dan jarak pandang yang jauh. Menggabungkan fitur mata secara eksplisit dengan atribut wajah lokal seperti tekstur kulit dan tanda wajah di daerah periokular (daerah di sekitar mata) dapat meningkatkan kinerja sistem biometrik berbasis wajah. Menggunakan iris dalam kerangka kerja multimoda dapat meningkatkan akurasi pencocokan dan mengurangi kendala pada kedalaman bidang dengan memungkinkan penggunaan gambar iris beresolusi rendah.

Penggunaan sistem biometrik dalam aplikasi pemerintah dan sipil berskala besar telah menimbulkan kekhawatiran tentang keamanan templat iris dan retensi privasi pemiliknya. Keamanan dan privasi menjadi perhatian khusus dalam basis data terpusat, yang dapat menyimpan jutaan templat iris. Teknologi peningkatan privasi, bersama dengan biometrik yang dapat dibatalkan (lihat Bab 7, Keamanan Sistem Biometrik), kemungkinan akan meningkatkan tingkat privasi dan keamanan informasi pribadi tersebut. Namun, penelitian lebih lanjut diperlukan untuk menggabungkan skema ini dalam lingkungan operasional.

Meskipun banyak tantangannya, pengenalan iris semakin populer sebagai teknologi biometrik yang tangguh dan andal. Tekstur iris yang kompleks dan stabilitasnya yang tampak menjanjikan untuk memanfaatkan pengenalan iris dalam berbagai skenario aplikasi, seperti kontrol perbatasan, investigasi forensik, dan kriptosistem. Penggunaan fitur mata dan atribut wajah lainnya bersama dengan modalitas iris dapat memungkinkan pengenalan biometrik dari jarak jauh dengan akurasi pencocokan yang sangat baik. Masa depan pengenalan berbasis iris tampak cerah, terutama dalam aplikasi militer yang menuntut identifikasi cepat individu dalam lingkungan yang dinamis.

BAB 5
CIRI-CIRI BIOMETRIK TAMBAHAN

Setiap sistem biometrik bergantung pada satu atau beberapa modalitas biometrik. Pilihan modalitas merupakan pendorong utama bagaimana sistem tersebut dirancang, bagaimana sistem tersebut disajikan kepada pengguna, dan bagaimana keputusan pencocokan vs. ketidakcocokan dibuat. Memahami modalitas tertentu dan cara terbaik untuk menggunakan modalitas tersebut sangat penting bagi efektivitas sistem secara keseluruhan.

Komite Biometrik Whither, Dewan Riset Nasional, 2010

Bab-bab sebelumnya dalam buku ini difokuskan secara eksklusif pada tiga modalitas biometrik tertentu - sidik jari, wajah, dan iris. Ciri-ciri ini telah dipelajari secara ekstensif dalam literatur dan telah dimasukkan dalam beberapa sistem biometrik pemerintah, militer, dan sipil di seluruh dunia. Namun, selain ciri-ciri ini, beberapa atribut biometrik lainnya juga telah dipelajari dalam konteks aplikasi mulai dari sistem kontrol perbatasan hingga pengawasan dan analisis forensik. Contoh atribut tersebut meliputi geometri tangan, telinga, ucapan, tanda tangan, gaya berjalan, DNA, dan gigi. Lebih jauh, atribut biometrik lunak (yaitu, atribut yang memberikan beberapa informasi tentang individu, tetapi tidak memiliki kekhasan dan keawetan untuk membedakan dua individu secara memadai) seperti bekas luka, tanda, dan tato (SMT), daerah periokular, dan metrologi manusia juga telah dipelajari dalam literatur biometrik. Bab ini akan memperkenalkan beberapa ciri ini untuk menyampaikan luasnya pekerjaan yang dilakukan di bidang biometrik.

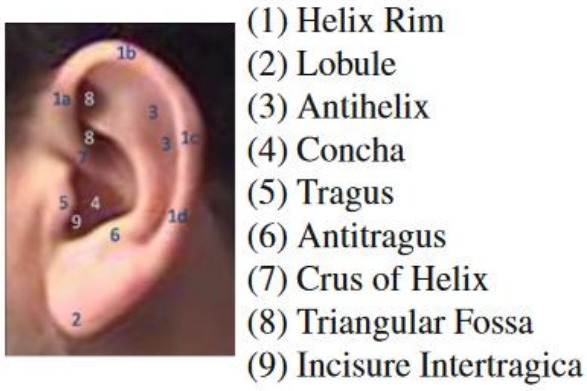
5.1 PENDAHULUAN

Seperti yang dinyatakan dalam Bab 1, berbagai macam ciri biometrik telah diusulkan dan dipelajari dalam literatur. Dalam beberapa kasus, keingintahuan akademis tentang keunikan dan keawetan ciri biologis tertentu telah memacu penelitian eksploratif (misalnya, iris); dalam kasus lain, domain aplikasi baru telah menghasilkan eksplorasi ciri biometrik baru (misalnya, biometrik periokular). Lebih jauh, ciri biometrik tertentu secara unik cocok untuk beberapa aplikasi dan skenario. Misalnya, suara mungkin lebih praktis dalam aplikasi tele-commerce; Telinga mungkin berguna dalam aplikasi pengawasan di mana hanya profil samping wajah manusia yang tersedia; pola gaya berjalan mungkin relevan dalam skenario identifikasi jarak jauh; geometri tangan mungkin sesuai untuk digunakan dalam sistem yang memerlukan verifikasi (bukan identifikasi) beberapa identitas yang terdaftar sehingga mengurangi beberapa masalah yang terkait dengan penggunaan isyarat biometrik yang kuat seperti sidik jari; dan iris atau sidik jari dapat dipilih dalam aplikasi di mana subjek kooperatif dan berada dalam jarak dekat dengan sensor.

Selain ciri-ciri yang disebutkan di atas, informasi tambahan seperti jenis kelamin, etnis, usia, tinggi badan, dan warna mata juga dapat digunakan untuk meningkatkan akurasi pencocokan sistem biometrik. Misalnya, jika subjek perempuan (probe) dicocokkan secara

tidak tepat dengan subjek laki-laki (di galeri), maka informasi jenis kelamin dapat digunakan oleh sistem biometrik untuk menolak pencocokan tersebut. Atribut tambahan memberikan informasi tambahan tentang individu, tetapi tidak memiliki kekhasan dan keawetan untuk membedakan dua individu secara memadai. Namun, atribut tersebut dapat digunakan untuk mempersempit ruang pencarian kecocokan potensial dalam sistem identifikasi (misalnya, jika probe input dianggap sebagai "Pria Asia", maka sistem identifikasi dapat membatasi pencariannya hanya pada identitas "Pria Asia" dalam basis data) atau ketika ciri biometrik lainnya tidak tersedia dengan mudah (misalnya, menggunakan informasi periokular ketika iris dianggap berkualitas buruk). Ciri-ciri tersebut umumnya disebut sebagai biometrik lunak dalam literatur. Tidak seperti beberapa atribut lain seperti sidik jari dan iris, ciri biometrik lunak tidak selalu "unik" bagi seorang individu. Ciri-ciri tersebut dapat dimiliki oleh sebagian besar populasi (misalnya, jenis kelamin) dan mungkin tidak permanen (misalnya, bekas luka, tanda, dan tato, disingkat SMT).

Mengingat keragaman ciri biometrik yang dibahas dalam literatur, demi kesingkatan, kami membatasi pembahasan kami pada empat ciri biometrik berikut dalam bab ini: telinga, gaya berjalan, geometri tangan, dan biometrik lunak.



Gambar 5.1 Anatomi luar telinga. Daun telinga yang terlihat sering disebut sebagai daun telinga. Struktur daun telinga yang rumit dan morfologinya diyakini unik bagi setiap individu, meskipun evaluasi skala besar terhadap sistem pengenalan telinga otomatis belum dilakukan.

5.2 DETEKSI TELINGA

Sejumlah teknik telah diusulkan untuk menemukan telinga dalam gambar tertentu. Pendekatan ini dapat dikategorikan ke dalam kelompok berikut.

1. **Pencocokan Templat:**
   Dalam skema pencocokan templat, templat telinga yang khas dibuat dan dicocokkan dengan setiap lokasi dalam gambar kueri. Lokasi yang memberikan skor tertinggi dianggap sebagai wilayah yang berisi telinga. Templat dapat terdiri dari gambar tepi telinga atau serangkaian deskriptor yang diekstraksi dari telinga seperti respons terhadap serangkaian filter atau histogram kelengkungan bentuk jika gambar 3D telinga digunakan untuk pengenalan. Deteksi berdasarkan respons terhadap

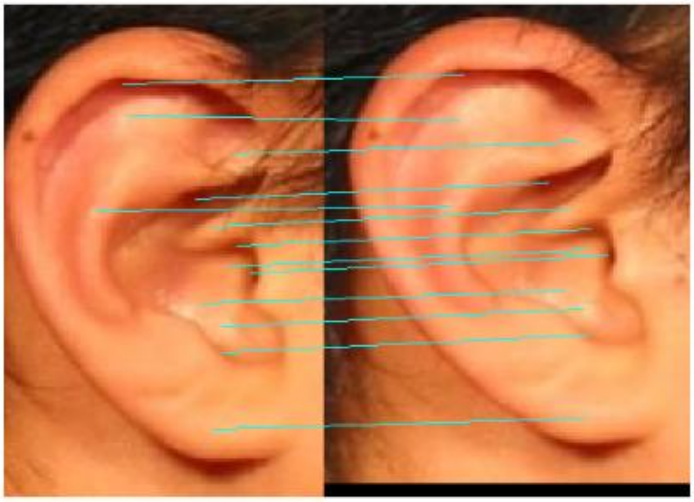
serangkaian filter yang telah dipilih sebelumnya, yang dikenal sebagai teknik Viola dan Jones, juga umum digunakan untuk mendeteksi wajah dalam gambar.

2. **Deteksi Berbasis Model:**
   Teknik deteksi berbasis model mengasumsikan karakteristik tertentu dari bentuk telinga dan mencoba menemukan wilayah yang menunjukkan karakteristik tersebut. Bentuk heliks, misalnya, biasanya elips sehingga transformasi Hough umum yang disetel untuk mendeteksi elips dapat digunakan untuk menemukan telinga dalam gambar tepi. Fitur yang diekstraksi menggunakan kode rantai1 juga dapat digunakan untuk mengklasifikasikan setiap kurva yang diperoleh dari gambar menjadi kurva yang terkait dengan telinga, seperti heliks atau anti-heliks.
3. **Deteksi Berbasis Operator Morfologi:**
   Karena struktur telinga biasanya lebih rumit daripada struktur wilayah yang tersisa dalam gambar profil wajah, transformasi morfologi seperti transformasi Top-hat dapat digunakan. Transformasi Top-hat pada dasarnya mengurangi versi gambar yang dihaluskan secara morfologis dari dirinya sendiri, sehingga menyorot detail yang lebih halus.
4. **Deteksi Berbasis Geometri Wajah:**
   Karena dalam gambar profil hidung dapat dengan mudah dideteksi sebagai titik dengan kelengkungan tinggi, maka dimungkinkan untuk membatasi pencarian telinga di lokasi yang tepat relatif terhadap hidung. Kinerja deteksi telinga dapat ditingkatkan dengan memanfaatkan pemrosesan dua tahap, di mana wilayah kulit disegmentasi dari gambar profil pada tahap pertama dan telinga dideteksi dalam ruang pencarian yang diperkecil ini selama tahap kedua.

Pengenalan telinga

1. **Teknik berbasis analisis subruang:**
   Mirip dengan pengenalan citra wajah, memproyeksikan citra telinga ke serangkaian arah utama merupakan cara yang efektif untuk memperoleh representasi telinga yang menonjol dan padat. Teknik proyeksi subruang seperti PCA, ICA, dan LDA telah berhasil digunakan dalam literatur untuk mencocokkan citra telinga. Lebih jauh, berbagai teknik berbasis pembelajaran seperti Locally Linear Embedding (LLE) dan Kernel PCA juga telah digunakan untuk melakukan pengenalan telinga.
2. **Teknik berbasis representasi renggang:**
   Teknik pengoptimalan yang meminimalkan norma L-1 dari vektor jarak antara kueri yang ditransformasikan dan semua templat yang ditransformasikan dalam basis data telah terbukti memberikan akurasi pengenalan yang tinggi dalam studi pengenalan objek. Teknik ini juga telah berhasil digunakan untuk pengenalan telinga.
3. **Teknik berbasis pencocokan himpunan titik:**
   Pencocokan graf ikatan elastis merupakan teknik yang efektif untuk mengenali wajah berdasarkan respons terhadap bank filter Gabor di beberapa titik fiducial pada wajah. Teknik ini juga telah berhasil digunakan untuk mencocokkan gambar telinga di mana sejumlah titik penting dapat dengan mudah dideteksi, berkat strukturnya yang

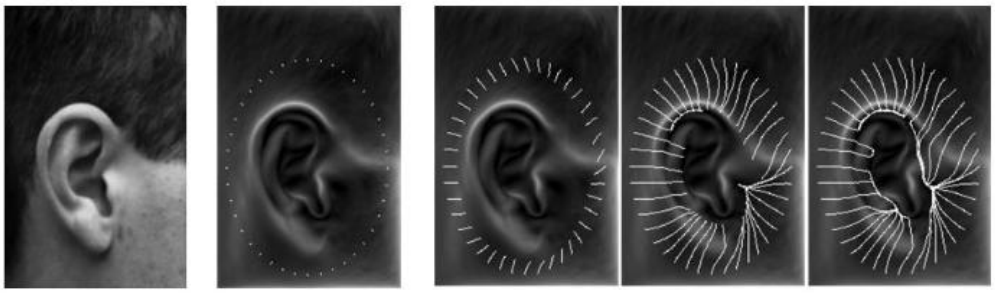
kompleks. *Scale Invariant Feature Transform* (SIFT) adalah teknik yang terkenal untuk mencocokkan dua gambar di mana serangkaian titik penting dapat diekstraksi darinya secara andal dan berulang. Untuk mencocokkan dua gambar menggunakan fitur SIFT, titik sudut dideteksi dari dua gambar dan dicocokkan berdasarkan fitur berbasis gradien gambar yang diekstraksi dari wilayah tetangga setiap titik. Lihat Gambar 5.2 untuk contoh titik SIFT yang dicocokkan antara dua gambar telinga.



Gambar 5.2 Membandingkan dua gambar telinga dengan menggunakan skema pencocokan titik kunci SIFT. Di sini, titik kunci SIFT pertama-tama diekstraksi dari setiap gambar sebelum membandingkannya.

4. **Teknik berbasis penyaringan gambar:**
   Dalam teknik tertentu, gambar telinga pertama-tama disempurnakan untuk menyorot fitur diskriminatif dan menekan noise. Dua teknik umum yang menggunakan prosedur dasar ini adalah transformasi medan gaya dan pola biner lokal.
   a. **Transformasi medan gaya:**
      Transformasi medan gaya pada dasarnya memperoleh intensitas gaya di setiap lokasi dalam gambar tempat setiap piksel dianggap sebagai sumber gaya dengan intensitas yang sebanding dengan nilainya. Transformasi medan gaya telah terbukti secara efektif menghilangkan derau dalam gambar telinga yang mengarah pada peningkatan signifikan dalam akurasi pengenalan. Lebih jauh, serangkaian garis yang menunjukkan gradien medan gaya ini dapat diekstraksi dan digunakan untuk pencocokan. Lihat Gambar 5.3 untuk penggambaran medan gaya yang diekstraksi dari gambar telinga dengan garis medan gaya yang ditandai.
   b. **Pola biner lokal:**
      Pola biner lokal pada dasarnya mengkarakterisasi setiap piksel berdasarkan variasi intensitas piksel tersebut di sepanjang serangkaian arah. Variasi di sepanjang setiap arah dikodekan sebagai satu bit yang menunjukkan apakah intensitas meningkat atau menurun, dan serangkaian bit yang terkait dengan

setiap arah digunakan untuk memperoleh nilai integer untuk setiap piksel. Transformasi semacam itu secara efektif mengurangi pengaruh variasi pencahayaan dan sumber noise lainnya, sehingga menghasilkan gambar yang ditingkatkan yang dapat digunakan untuk pencocokan yang kuat.



Gambar 5.3 Ekstraksi garis medan gaya dari gambar telinga menggunakan pendekatan iteratif.

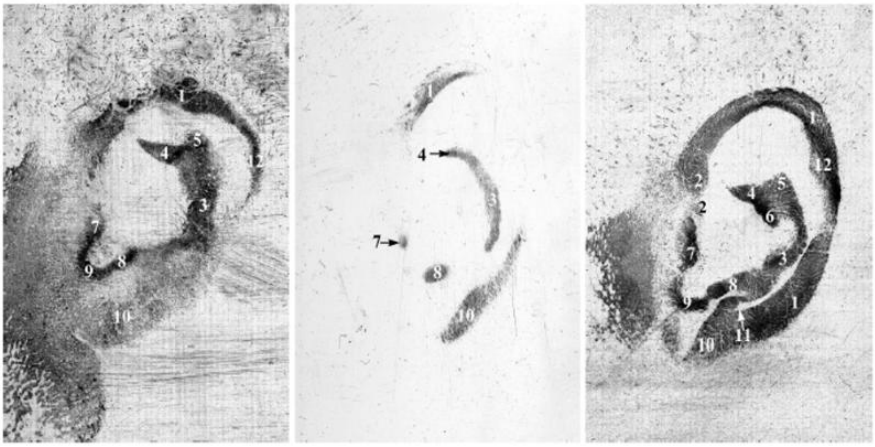
5. **Teknik berbasis pengukuran geometris:**
   Fitur yang diperoleh dengan mengukur karakteristik geometris tertentu dari telinga juga dapat digunakan sebagai serangkaian fitur diskriminatif. Sebagai contoh, titik berat gambar telinga yang diperoleh dari gambar tepinya dapat digunakan sebagai pusat untuk menggambar lingkaran konsentris dengan jari-jari yang telah ditentukan sebelumnya. Berbagai pengukuran, seperti jumlah titik pada lingkaran yang memotong gambar tepi atau jarak antara dua perpotongan yang berurutan, dapat digunakan sebagai vektor fitur. Karakteristik kurva yang berbeda yang ada dalam gambar tepi seperti koordinat ujung dan percabangan juga dapat digunakan sebagai fitur tambahan.
6. **Teknik berbasis transformasi:**
   Berbagai teknik transformasi gambar seperti transformasi Fourier atau transformasi wavelet juga dapat diterapkan untuk mengekstraksi fitur diskriminatif dari gambar telinga. Transformasi Fourier juga dapat diterapkan untuk memperoleh representasi telinga yang invarian terhadap rotasi dan translasi - misalnya, dengan menggunakan sistem koordinat polar dan mengekstraksi hanya besarnya transformasi Fourier.
7. **Teknik 3D:**
   Dalam beberapa skenario, memperoleh tampilan entitas telinga dalam 3D mungkin dapat dilakukan. Citra 3D menawarkan informasi kedalaman yang dapat digunakan bersama dengan informasi tekstur 2D untuk meningkatkan akurasi pengenalan. Dalam kasus citra telinga 3D, histogram lokal dari nilai kelengkungan bentuk dapat digunakan untuk mencocokkan dua citra telinga. Algoritma Iterative Closest Point (ICP) umumnya digunakan untuk mendaftarkan dan mencocokkan telinga 3D. Dalam teknik ICP, setiap titik dalam citra telinga input digunakan untuk memperoleh titik yang sesuai dalam citra templat dan input kemudian diputar dan ditranslasi untuk meminimalkan jarak antara titik yang sesuai. Prosedur ini diterapkan secara iteratif

hingga konvergensi, dan kumpulan jarak yang dihasilkan digunakan untuk menghitung skor pencocokan.

Tantangan dalam pengenalan telinga

Meskipun beberapa algoritme untuk pendeteksian dan pencocokan telinga telah diusulkan dalam literatur, evaluasi publik berskala besar terhadap algoritme pengenalan telinga belum dilakukan. Lebih jauh, saat ini tidak ada sistem biometrik komersial yang secara eksplisit memanfaatkan fitur telinga untuk pengenalan manusia. Namun, kinerja algoritme pengenalan telinga telah diuji pada beberapa set data telinga standar. Eksperimen menunjukkan bahwa gambar telinga yang diperoleh dalam kondisi terkendali dapat menghasilkan akurasi pengenalan yang baik. Namun, kinerja metode pengenalan telinga pada gambar non-ideal yang diperoleh dalam berbagai kondisi pencahayaan dan oklusi belum ditetapkan. Beberapa tantangan harus diatasi untuk memungkinkan hal ini.

1. **Oklusi Telinga:**
   Salah satu tantangan utama yang dihadapi oleh sistem pengenalan telinga adalah oklusi akibat rambut subjek. Salah satu cara untuk mengatasi oklusi tersebut adalah dengan menangkap termogram bersama dengan gambar cahaya tampak. Dalam termogram, rambut dapat dengan mudah dideteksi (dan mungkin diisolasi) karena suhunya biasanya lebih rendah daripada suhu kulit.
2. **Identifikasi Jejak Telinga:**
   Jejak telinga, atau tanda telinga, adalah tanda yang ditinggalkan oleh sekresi akibat menekan telinga ke permukaan yang datar. Tanda-tanda ini terutama terdiri dari cetakan heliks, anti-heliks, tragus, dan anti-tragus. Fitur lainnya termasuk cuping telinga dan krus heliks, tetapi lebih jarang diamati. Jejak telinga dapat dibandingkan berdasarkan detail seperti takik dan sudut pada sampel yang dicetak, posisi tahi lalat, lipatan, dan kerutan, serta posisi titik-titik tekanan. Gambar 5.4 memberikan serangkaian contoh jejak telinga yang diambil dari tempat kejadian perkara.



Gambar 5.4 Contoh-contoh sidik telinga yang menunjukkan berbagai ciri anatomi. Label-label dalam gambar ini adalah sebagai berikut: 1. heliks; 2. krus heliks; 3-6. bagian-bagian anti-heliks; 7. tragus; 8. antitragus; 9. incisura intertragis; 10. lobus.

Sidik telinga diketahui tersedia pada sekitar 15% kasus kejahatan dan juga telah dipertimbangkan dalam beberapa kasus pengadilan sebagai sumber bukti forensik. Namun, karena variasi yang signifikan di antara beberapa cetakan telinga, individualisasi berdasarkan jejak telinga sering kali diperdebatkan. Alasan utama yang membingungkan individualisasi sidik telinga meliputi (a) deformasi variabel yang disebabkan oleh gaya yang diberikan oleh telinga ke permukaan, (b) durasi kontak telinga dengan permukaan, (c) modifikasi ornamen pada telinga, seperti tindik, dan (d) perubahan bentuk dan ukuran telinga karena penuaan. Identifikasi sidik telinga biasanya dilakukan secara manual dengan mengidentifikasi dan mencocokkan serangkaian fitur geometris dari sidik telinga seperti titik potong lengkung telinga dengan kisi-kisi biasa atau lokasi titik acuan tertentu lainnya. Sistem yang sepenuhnya otomatis yang memanfaatkan fitur SIFT juga telah dirancang untuk mencocokkan dua sidik telinga, tetapi kinerjanya belum dievaluasi secara ekstensif dalam lingkungan operasional.

5.3 GAYA BERJALAN

Permintaan untuk identifikasi manusia dari jarak jauh telah memperoleh daya tarik yang cukup besar, terutama karena kebutuhan untuk mengenali individu secara diam-diam di lingkungan yang tidak terbatas dengan subjek yang tidak kooperatif. Di lingkungan seperti itu, orang yang dimaksud mungkin tidak berinteraksi dengan sistem biometrik secara terpadu. Lebih jauh, individu tersebut mungkin bergerak di lingkungan ini yang dicirikan oleh pencahayaan yang bervariasi dan latar belakang yang tidak seragam. Modalitas biometrik seperti sidik jari dan iris tidak dapat diperoleh dengan mudah pada jarak yang jauh. Sebaliknya, modalitas wajah dan gaya berjalan dapat diperoleh dengan mudah dari jarak jauh, meskipun resolusi spasial wajah yang lebih kecil pada jarak yang jauh dapat menurunkan akurasi sistem pengenalan wajah. Akibatnya, pengenalan manusia berbasis gaya berjalan telah menarik minat untuk pengenalan biometrik dari jarak jauh.

Gaya berjalan didefinisikan sebagai pola pergerakan pada hewan. Oleh karena itu, gaya berjalan manusia adalah cara orang berjalan. Sementara definisi formal gaya berjalan mengacu pada gerakan manusia, algoritme praktis untuk pengenalan gaya berjalan mencakup fitur dinamis dan statis (seperti bentuk tubuh) dari tubuh manusia yang bergerak. Hal ini dapat dilihat sebagai sifat perilaku yang dipengaruhi oleh struktur muskuloskeletal tubuh manusia. Pengenalan gaya berjalan dianggap sebagai solusi yang menarik untuk identifikasi berbasis jarak karena sejumlah alasan. Pertama dan yang terpenting, gaya berjalan manusia telah diamati memiliki beberapa karakteristik khusus orang. Studi psikologis oleh Cutting dan Kozlowski menunjukkan bahwa manusia mampu menyimpulkan jenis kelamin dan mengenali individu yang dikenal berdasarkan gaya berjalan. Kedua, biometrik gaya berjalan dapat diperoleh secara pasif dan, oleh karena itu, interaksi subjek yang eksplisit tidak diperlukan untuk perolehan data. Pengumpulan data secara pasif bermanfaat dalam lingkungan tempat subjek diamati secara diam-diam. Terakhir, fitur diskriminatif gaya berjalan manusia dapat diekstraksi dalam gambar beresolusi rendah. Hal

ini menunjukkan bahwa sistem kamera yang mahal mungkin tidak diperlukan untuk pengenalan gaya berjalan.

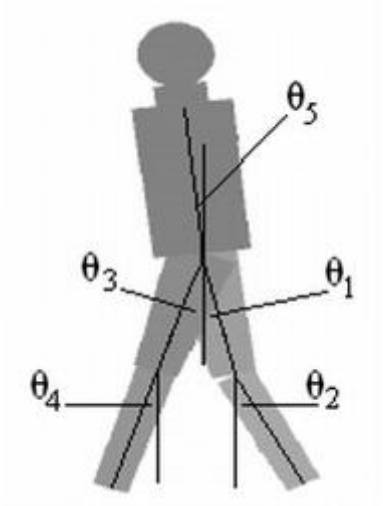
Biasanya, algoritma untuk pengenalan gaya berjalan dimulai dengan proses ekstraksi siluet. Komponen ini bertujuan untuk mengisolasi (yaitu, menyegmentasikan atau melokalisasi) kontur tubuh manusia dari rangkaian video. Metode sederhana untuk mencapai hal ini adalah melalui pengurangan latar belakang, berdasarkan bingkai per bingkai, meskipun metode yang lebih canggih berdasarkan Model Campuran Gaussian dan Medan Ukur Markov Tersembunyi juga ada. Setelah siluet ditentukan, fitur dapat diekstraksi untuk pemrosesan lebih lanjut. Metode untuk ekstraksi fitur biasanya berbasis model atau bebas model.

Pendekatan berbasis model menggabungkan informasi struktural tubuh manusia baik berdasarkan informasi apriori atau melalui model tubuh manusia yang disimpulkan dari data pelatihan. Berbagai macam model biped3 umumnya digunakan, meskipun bervariasi dalam hal kompleksitas dan informasi yang diekstraksi. Manfaat dari pendekatan berbasis model adalah bahwa model yang baik memungkinkan ekstraksi fitur yang kuat dan konsisten. Karena fitur diperoleh dari informasi struktural, distorsi dalam bentuk siluet cenderung tidak menyebabkan kesalahan. Di sisi lain, pendekatan bebas model umumnya bertujuan untuk mengekstraksi fitur berdasarkan pergerakan siluet seiring waktu. Keuntungan utama dari pendekatan bebas model adalah kesederhanaan komputasi, karena banyak algoritme kelas ini dapat dieksekusi dengan cepat. Namun, masalah yang sering dikutip dari algoritme bebas model adalah ketidakmampuannya untuk beradaptasi dengan distorsi siluet yang timbul dari variasi sudut pandang kamera dan pakaian, atau kesalahan dalam segmentasi. Di bagian berikut, dua algoritme populer untuk ekstraksi fitur akan dibahas secara singkat.

1) Kode rantai biasanya mengukur orientasi lokal sepanjang kurva.
2) Jarak antara subjek dan perangkat akuisisi disebut sebagai jarak berdiri.
3) Model biped adalah model berkaki dua.

Ekstraksi dan pencocokan fitur

Contoh pendekatan berbasis model adalah model biped lima tautan yang digunakan untuk merepresentasikan pergerakan manusia. Model ini dirancang untuk merepresentasikan gaya berjalan melintasi bidang sagital (profil samping) dan ditunjukkan pada Gambar 5.5.



Gambar 5.5 Model biped lima-tautan yang digunakan untuk memodelkan tubuh manusia untuk pengenalan gaya berjalan.

Dengan menyertakan koordinat centroid, (x, y), model tersebut terdiri dari 7 parameter. Masing-masing dari lima sudut tersebut dilambangkan sebagai sudut elevasi bidang sagital (SEA) dan didefinisikan sebagai sudut antara sumbu utama bagian tubuh dan sumbu y. Setiap komponen model juga didefinisikan oleh komponen tinggi (l), dan panjang alas atas dan bawah (t dan b). Dengan menggunakan $\alpha = t/l$ dan $\beta = b/l$, setiap bagian $p_1, i = 1, \dots, 5$ direpresentasikan sebagai $p_1 = \{\alpha_1, \beta_1, l_1$. Tinggi bagian tersebut selanjutnya dinormalisasi terhadap batang tubuh (l5) untuk memperoleh invariansi skala. Model lengkap didefinisikan sebagai berikut:

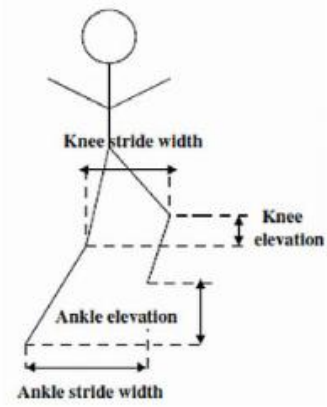
$$H = \{K, R, M\} \tag{5.1}$$

$$K = \{\alpha_1, \beta_1, \alpha_2, \beta_2, \dots, \alpha_5\beta_5\} \tag{5.2}$$

$$R = \{r_1, r_2 \dots, r_5\}, r_1 = l_1/l_5 \tag{5.3}$$

$$M = \{x, y, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5\}p_1 \tag{5.4}$$

Dengan menggunakan parameter di atas, fitur domain ruang dihitung untuk pengenalan. Fitur ini meliputi elevasi pergelangan kaki (s_1), elevasi lutut (s_2), lebar langkah pergelangan kaki (3), dan lebar langkah lutut (s_4). Transformasi Fourier Diskrit dihitung untuk setiap fitur ini dan kemudian digunakan sebagai vektor fitur utama untuk pengenalan. Ilustrasi fitur ini disediakan pada Gambar 5.6.



Gambar 5.6 Fitur domain ruang yang diekstrak dari model biped lima tautan.

Pendekatan bebas model

Mungkin pendekatan bebas model yang paling populer adalah algoritma Gait Energy Image (GEI). Meskipun tidak menghasilkan kinerja pencocokan yang unggul, algoritma ini sering dikutip sebagai tolok ukur untuk perbandingan karena kemudahan implementasinya. GEI bertujuan untuk mengukur dinamika gaya berjalan seseorang melalui representasi berbasis gambar tunggal. Diberikan N gambar siluet biner, $S_t(x, y)$, pada berbagai contoh waktu yang dilambangkan dengan t, gambar energi gaya berjalan didefinisikan sebagai:

$$G(x, y) = \frac{1}{N}\sum_{t=1}^{N} S_t(x, y) \tag{5.5}$$

Singkatnya, Persamaan (5.5) menggambarkan intensitas siluet yang dirata-ratakan pada N bingkai. Sebelum dirata-ratakan, gambar harus dinormalisasi sedemikian rupa sehingga tinggi setiap siluet sama. Selain itu, gambar harus disejajarkan menurut centroid horizontal. Penyelarasan horizontal memungkinkan dinamika bentuk bergerak divisualisasikan dalam gambar akhir. Contoh diberikan pada Gambar 5.7. Di sini, gambar paling kanan di setiap baris menggambarkan gambar energi gaya berjalan.

Gambar. 5.7 Contoh yang menunjukkan bingkai siluet yang dinormalkan beserta gambar energi gaya berjalan (GEI). Dua baris tersebut sesuai dengan dua subjek yang berbeda. Di setiap baris, 7 bingkai digunakan untuk memperoleh GEI yang merupakan gambar paling kanan.

Untuk setiap gambar energi gaya berjalan, dinamika gaya berjalan ditangkap dalam hal intensitas piksel. Gambar energi diubah menjadi vektor fitur dan digunakan untuk pengenalan gaya berjalan.

Pencocokan fitur

Vektor fitur yang dihasilkan yang dibangun menggunakan metode yang diuraikan di atas sering kali menghasilkan dimensionalitas yang besar, yang sulit untuk diklasifikasikan, terutama ketika jumlah sampel pelatihan kecil. Biasanya, kombinasi Analisis Komponen Utama (PCA) dan Analisis Diskriminan Linier (LDA) digunakan untuk pengurangan dimensionalitas dan pengoptimalan subruang. Vektor fitur yang direduksi kemudian dibandingkan menggunakan metrik jarak Euclidean.

Tantangan dalam pengenalan gaya berjalan

Kinerja pencocokan algoritma pengenalan gaya berjalan dipengaruhi oleh faktor-faktor seperti pakaian, alas kaki, permukaan jalan, kecepatan berjalan, arah berjalan (sehubungan dengan kamera), dll. Lebih jauh, pola gaya berjalan seseorang dapat berubah seiring waktu, terutama dengan variasi massa tubuh. Dampak dari faktor-faktor ini sulit dikurangi dan, oleh karena itu, evaluasi algoritma pengenalan gaya berjalan sebagian besar dilakukan di lingkungan yang terkendali. Hal ini telah mencegah penggabungan pengenalan gaya berjalan dalam sistem biometrik komersial.

5.4 GEOMETRI TANGAN

Geometri tangan, seperti namanya, mengacu pada struktur geometris tangan. Struktur ini meliputi lebar jari di berbagai lokasi, lebar telapak tangan, ketebalan telapak tangan, panjang jari, kontur telapak tangan, dll. Meskipun metrik ini tidak bervariasi secara signifikan di seluruh populasi, metrik ini tetap dapat digunakan untuk memverifikasi identitas seseorang. Pengukuran geometri tangan bersifat non-intrusif dan verifikasi melibatkan pemrosesan sederhana dari fitur yang dihasilkan. Tidak seperti sidik telapak tangan, metode ini tidak melibatkan ekstraksi fitur tangan secara terperinci (misalnya, kerutan pada kulit).

Sistem verifikasi berbasis geometri tangan telah tersedia secara komersial sejak awal 1970-an. Literatur paling awal tentang biometrik geometri tangan berbentuk paten atau deskripsi berorientasi aplikasi. Sidlauskas memperkenalkan peralatan identifikasi profil tangan 3D yang berhasil digunakan untuk pengenalan geometri tangan. Sistem geometri tangan telah digunakan di beberapa pembangkit listrik tenaga nuklir di seluruh Amerika Serikat. Selain itu, kios geometri tangan tersedia di bandara Ben Gurion (Tel Aviv, Israel) untuk verifikasi cepat para pelancong yang sering bepergian.

Sistem geometri tangan yang umum terdiri dari empat komponen utama: akuisisi gambar, segmentasi dan penyelarasan tangan, ekstraksi fitur, dan pencocokan fitur.

Pengambilan gambar

Kebanyakan sistem geometri tangan mengambil gambar bagian belakang tangan manusia. Gambar ini sering disebut sebagai aspek punggung tangan. Dengan demikian,

sebagian besar sistem komersial mengharuskan subjek untuk meletakkan tangannya di atas pelat dengan telapak tangan menghadap ke bawah. Kamera yang diposisikan dengan tepat di atas tangan kemudian digunakan untuk mengambil gambar aspek punggung tangan. Berbagai jenis konfigurasi pencitraan telah dibahas dalam literatur geometri tangan seperti yang dijelaskan di bawah ini.

1. Berbasis Kontak vs Tanpa Kontak: Sistem yang umum mengharuskan pengguna untuk meletakkan tangannya di permukaan yang datar sebelum mengambil gambar. Sistem semacam itu berbasis kontak dan memerlukan kerja sama eksplisit dari subjek yang diidentifikasi. Namun, kebersihan merupakan masalah yang menjadi perhatian beberapa pengguna dalam sistem semacam itu. Lebih jauh, ukuran tangan yang besar (dibandingkan dengan, katakanlah, jari) membatasi penggunaan sistem geometri tangan pada perangkat yang lebih kecil (misalnya, ponsel). Untuk mengatasi masalah ini, sistem pengenalan nirkontak telah diusulkan. Namun, sistem semacam itu diperlukan untuk mengatasi variabilitas intrakelas dalam gambar yang diambil karena artikulasi tangan dalam ketiga dimensi.
2. Dorsal vs Palmar: Secara tradisional, gambar tangan diperoleh dengan meletakkan tangan pada permukaan datar dan mengambil gambar bagian belakang tangan dengan kamera CCD. Namun, ada minat untuk menangkap pola tonjolan yang ada di telapak tangan dan jari beserta bentuk tangan dengan mengambil gambar aspek palmar tangan (termasuk telapak bagian dalam). Lihat Gambar 5.8 (b) sebagai contoh. Salah satu kelemahan sistem semacam itu adalah agak merepotkan bagi pengguna untuk meletakkan tangan di atas platen dengan telapak tangan menghadap ke atas.
3. Berbasis pasak vs Tanpa pasak: Untuk memandu posisi tangan di platen untuk keperluan pencitraan (misalnya, untuk mencegah jari-jari saling bersentuhan), beberapa pasak biasanya diletakkan di platen sensor. Lihat Gambar 5.8 (a). Pengguna diharapkan menggerakkan tangannya ke depan hingga salah satu pasak menyentuh anyaman di antara sepasang jari. Meskipun penggunaan pasak meniadakan perlunya penyelarasan gambar, hal itu menambah kerumitan penggunaan sistem dan, dengan demikian, menambah ketidaknyamanan bagi pengguna. Lihat Gambar 5.9 untuk contoh di mana pengguna salah meletakkan jari-jarinya di sekitar pasak.

(a) (b)

Gambar 5.8 Berbagai konfigurasi pencitraan untuk memperoleh sampel tangan manusia. a) Skenario penangkapan tangan yang dibatasi. b) Skenario penangkapan yang tidak dibatasi.

Gambar 5.9 Contoh yang menunjukkan penempatan tangan yang salah dalam sistem berbasis pasak.

Segmentasi tangan

Setelah gambar tangan diambil, batas tangan harus diekstraksi untuk menentukan wilayah yang diinginkan. Untuk mencapai hal ini, biasanya, gambar tersebut diambang batas

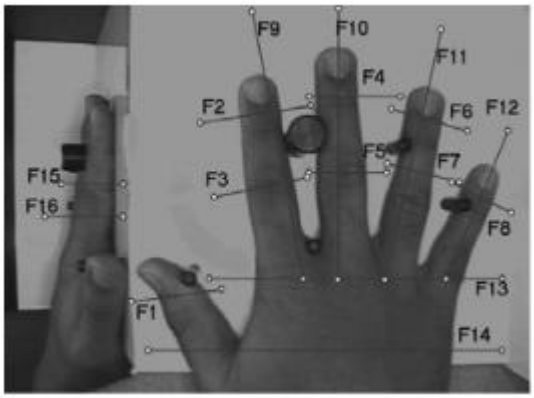
untuk menyimpulkan wilayah yang terkait dengan tangan. Ini diikuti oleh operator morfologi tertentu (misalnya, dilatasi dan erosi diikuti oleh analisis wilayah terhubung) untuk mengekstrak siluet tangan. Jika gambar sangat bising (misalnya, karena pencahayaan dan bayangan yang bervariasi), maka teknik segmentasi yang lebih kompleks seperti algoritma pergeseran rata-rata mungkin diperlukan.

Tangan yang disegmentasi mungkin masih berisi beberapa artefak seperti pasak pada platen, cincin yang dikenakan oleh pengguna, pakaian yang menutupi bagian-bagian tertentu dari tangan, dan kontur terputus-putus karena pencahayaan yang tidak seragam. Artefak ini dihilangkan menggunakan teknik pemrosesan gambar khusus yang disesuaikan dengan artefak tertentu. Setelah bentuk tangan yang andal diperoleh, kontur tangan diekstraksi dan digunakan untuk pemrosesan lebih lanjut.

Karena adanya variasi dalam cara pengguna meletakkan tangan mereka, siluet yang diekstraksi dari beberapa tangkapan tangan yang sama mungkin tidak sejajar secara tepat. Penting untuk memperhitungkan variasi ini sebelum mengekstraksi fitur, terutama jika fitur tersebut tidak invarian terhadap transformasi geometris tersebut. Seperangkat transformasi yang umum mencakup rotasi dan translasi tangan, dan gerakan jari-jari individual. Lebih mudah untuk memperhitungkan transformasi afinitas global seperti translasi atau rotasi seluruh tangan, sementara mengakomodasi gerakan satu jari secara otomatis relatif sulit. Untuk memperbaiki situasi ini, tangan yang tersegmentasi dapat dibagi lebih lanjut untuk mendapatkan segmen yang lebih kecil yang sesuai dengan jari-jari individual. Fitur kemudian dapat diekstraksi secara terpisah dari masing-masing segmen ini.

Ekstraksi Fitur

Biasanya, dua jenis fitur diekstraksi dari siluet tangan atau jari: pengukuran geometris satu dimensi dan fitur berbasis bentuk dua dimensi. Pengukuran geometris meliputi panjang dan lebar jari, panjang dan lebar telapak tangan, dan ketebalan jari. Lihat Gambar 5.10 untuk contoh pengukuran geometris yang diperoleh dari gambar tangan.



Gambar 5.10 Gambar ini mengilustrasikan sumbu-sumbu yang digunakan untuk mengekstraksi ukuran geometris gambar tangan. Seperti yang dapat dilihat di sini,

Ukuran geometris meliputi panjang jari, lebar jari, lebar telapak tangan, dan kedalaman tangan. Meskipun ukuran individual mungkin tidak cukup diskriminatif untuk

pengenalan biometrik, pengelompokan ukuran ini menghasilkan vektor fitur yang dapat digunakan secara efektif untuk verifikasi biometrik.

Seperangkat titik di sepanjang kontur siluet (atau gambar tersegmentasi itu sendiri) juga dapat digunakan sebagai fitur. Dimensionalitas fitur ini dapat dikurangi untuk mendapatkan representasi tangan yang lebih diskriminatif dan ringkas. Fitur berbasis bentuk seperti itu diharapkan lebih diskriminatif daripada fitur geometris karena fitur tersebut memodelkan struktur seluruh tangan, bukan bagian-bagian tangan, sehingga memanfaatkan lebih banyak informasi.

Pencocokan fitur

Fitur yang diekstraksi dari gambar tangan tersegmentasi sering kali dapat dilambangkan sebagai vektor fitur dalam ruang Euclidean. Akibatnya, ukuran jarak umum seperti jarak Euclidean dan Manhattan dapat digunakan secara efektif untuk membandingkan dua gambar tangan. Jika jumlah data pelatihan yang tersedia mencukupi, ukuran jarak yang lebih canggih seperti jarak Mahalanobis juga dapat digunakan untuk pencocokan yang kuat. Jika pengambilan sampel titik-titik pada siluet digunakan secara langsung untuk pencocokan, maka pengukuran jarak seperti jarak Hausdorff dapat digunakan untuk memperoleh skor pencocokan. Dimungkinkan juga untuk menggunakan skema pembelajaran mesin untuk merancang pengklasifikasi seperti Support Vector Machines (SVM) multikelas yang dapat memetakan set fitur input ke dalam satu dari banyak identitas.

Tantangan dalam pengenalan geometri tangan

Sistem geometri tangan telah berhasil diterapkan dalam beberapa aplikasi, termasuk pembangkit listrik tenaga nuklir, sistem kontrol perbatasan, pusat rekreasi, dan sistem waktu dan kehadiran. Dalam aplikasi ini, sistem biometrik biasanya beroperasi dalam mode verifikasi. Karena geometri tangan sebagian individu dapat serupa, akurasi identifikasi karena modalitas biometrik ini dapat rendah. Lebih jauh, bentuk tangan individu dapat berubah seiring waktu - faktor yang terutama terlihat pada anak kecil. Penelitian yang lebih baru telah mengeksplorasi penggunaan geometri tangan bersama dengan sidik jari dan telapak tangan beresolusi rendah dalam konfigurasi multibiometrik untuk meningkatkan akurasi.

5.5 BIOMETRIK LUNAK

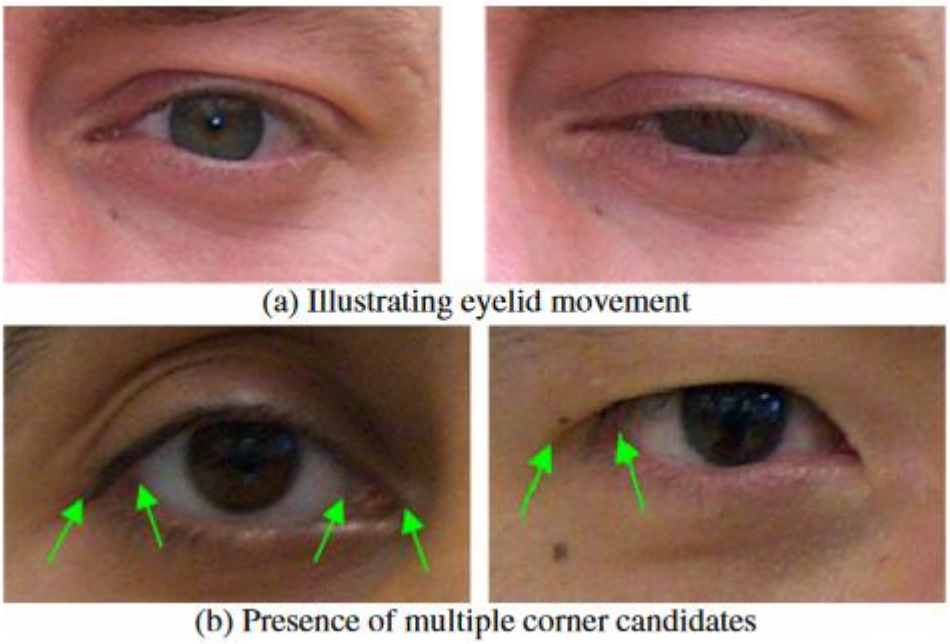
Ada banyak situasi di mana ciri biometrik utama (misalnya, wajah, sidik jari, dan iris) rusak atau tidak tersedia, dan informasi biometrik lunak adalah satu-satunya petunjuk yang tersedia untuk memecahkan kejahatan. Misalnya, meskipun video pengawasan mungkin tidak menangkap wajah tersangka secara keseluruhan, gambar wajah dalam video tersebut dapat mengungkapkan jenis kelamin dan etnis tersangka, atau adanya tanda atau tato dapat memberikan petunjuk berharga tambahan. Kami akan membahas beberapa ciri biometrik lunak (yaitu, periokular, tanda wajah, dan tato) di bawah ini. Biometrik periokular semakin mendapat perhatian karena menawarkan pilihan antara menggunakan seluruh gambar wajah dan hanya bagian iris. Tanda wajah dan tato juga semakin mendapat perhatian karena

menawarkan informasi pelengkap yang dapat dimanfaatkan bersama dengan ciri biometrik primer.

Periokular

Wilayah periokular merupakan wilayah di sekitar mata. Wilayah ini sebagian besar terdiri dari kulit, alis, dan mata. Penggunaan wilayah periokular sebagai isyarat biometrik merupakan pilihan yang tepat antara menggunakan seluruh wilayah wajah atau hanya menggunakan iris untuk pengenalan. Ketika seluruh wajah dicitrakan dari jarak jauh, informasi iris biasanya beresolusi rendah; ini berarti kinerja pencocokan karena modalitas iris akan buruk. Di sisi lain, ketika iris dicitrakan pada jarak yang kecil (biasanya, 1 meter), seluruh wajah mungkin tidak tersedia, sehingga memaksa sistem pengenalan hanya mengandalkan iris. Namun, biometrik periokular dapat digunakan untuk berbagai jarak. Gambar 5.11 menunjukkan contoh gambar periokular yang dikumpulkan dari dua subjek yang berbeda. Gambar periokular juga dapat diambil dalam spektrum NIR untuk meminimalkan variasi iluminasi dibandingkan dengan spektrum tampak. Langkah-langkah utama dalam praproses, ekstraksi fitur, dan pencocokan gambar periokular pita tampak dijelaskan di bawah ini.

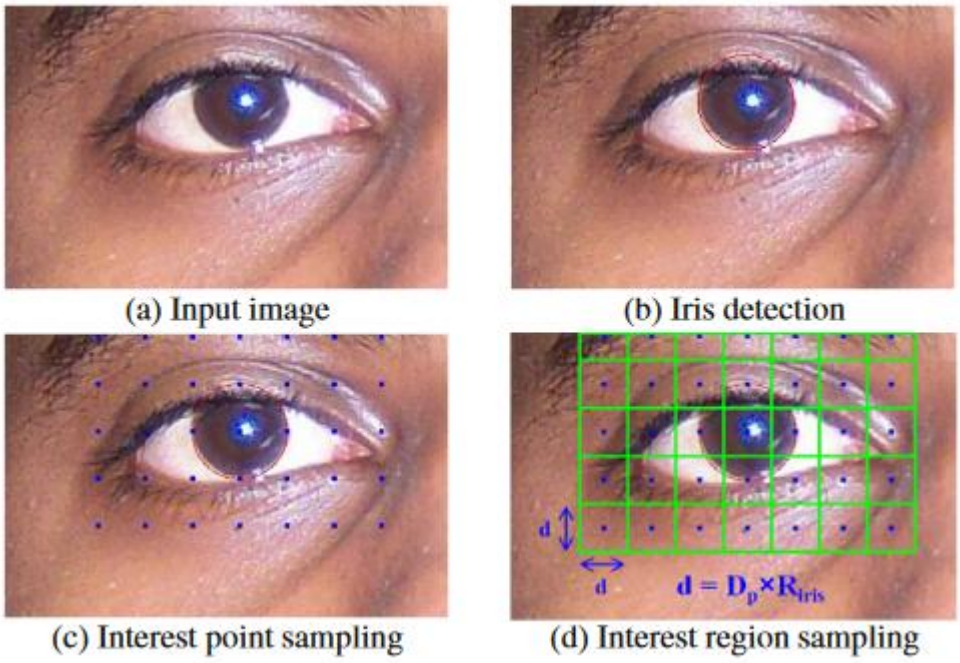
Gambar 5.11 Contoh gambar periokular dari dua subjek yang berbeda.



Gambar 5.12 Contoh gambar yang menunjukkan kesulitan dalam penyelarasan gambar periokular.

Prapemrosesan

Gambar periokular mengandung komponen umum di seluruh gambar (misalnya, iris, sklera, dan kelopak mata) yang dapat direpresentasikan dalam sistem koordinat umum. Setelah area minat umum dilokalisasi, skema representasi fitur global dapat digunakan. Skema representasi global bersifat holistik karena mengkarakterisasi seluruh wilayah periokular, bukan hanya wilayah lokal. Iris atau kelopak mata adalah kandidat yang baik untuk proses penyelarasan. Sementara deteksi iris dapat dilakukan dengan cukup baik karena geometri iris yang hampir melingkar dan kontras yang baik antara iris dan sklera, mendeteksi kelopak mata secara akurat lebih sulit. Sudut dalam dan luar mata juga dapat dianggap sebagai titik referensi, tetapi dapat ada beberapa kandidat seperti yang ditunjukkan pada Gambar 5.12. Oleh karena itu, kami akan membahas metode penyelarasan gambar berbasis iris di bagian ini. Iris dapat digunakan untuk translasi dan normalisasi skala gambar, tetapi tidak untuk normalisasi rotasi. Namun, variasi rotasi kecil dapat diatasi dengan menggunakan representasi fitur yang toleran terhadap rotasi dalam tahap ekstraksi fitur.



Gambar 5.13 Skema penyelarasan gambar dan proses ekstraksi fitur untuk gambar periokular.

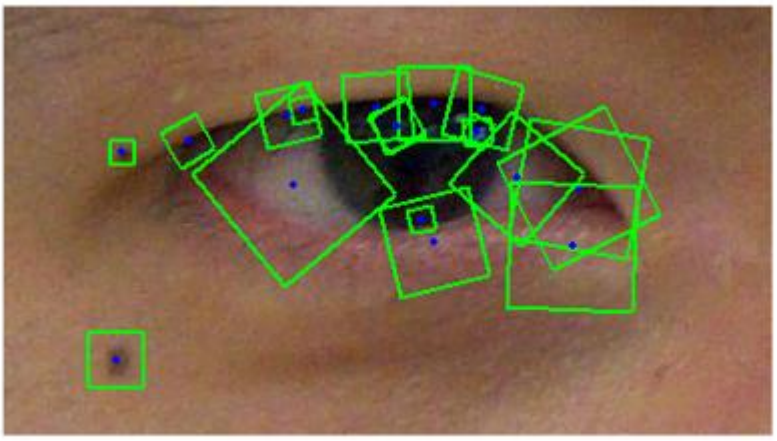
Ekstraksi fitur

Fitur dapat diekstraksi menggunakan semua nilai piksel di wilayah minat yang ditetapkan sehubungan dengan iris. Dari pusat, C_{iris}, dan radius, C_{iris}, iris, beberapa ($= n_{np}$) titik minat p_1, p_2, p_{npi} dipilih dalam jendela persegi panjang yang ditetapkan di sekitar Ciris dengan lebar $6 \times R_{iris}$ dan tinggi $4 \times R_{iris}$ seperti yang ditunjukkan pada Gambar 5.13. Jumlah titik minat diputuskan berdasarkan frekuensi pengambilan sampel ($1 \times D_p$), yang

berbanding terbalik dengan jarak antara titik minat, $D_p \times R_{iris}$. Untuk setiap titik minat p_i, wilayah persegi panjang r_i ditetapkan. Dimensi setiap persegi panjang (r) dalam ROI berukuran ($D_p \times R_{iris}$) dengan ($D_p \times R_{iris}$). Bila $D_p = 1$, ukuran persegi panjang menjadi $R_{iris} \times R_{iris}$ (lihat Gambar 5.13 (d)).

Untuk konstruksi deskriptor di setiap wilayah, ri, beberapa deskriptor berbasis distribusi seperti histogram orientasi gradien (GO) dan pola biner lokal (LBP) dapat digunakan. Respons GO dan LBP dikuantisasi menjadi 8 nilai berbeda untuk membangun histogram delapan bin di setiap subwilayah. Histogram delapan bin dibangun dari subwilayah yang dipartisi dan dirangkai di berbagai subwilayah untuk membangun vektor fitur. Gaussian blurring dengan deviasi standar, σ, dapat diterapkan sebelum mengekstraksi fitur menggunakan metode GO dan LBP untuk menghaluskan variasi di seluruh nilai piksel lokal.

Sebagai alternatif, serangkaian titik kunci yang menonjol dapat dideteksi dalam ruang skala mengikuti metode Scale Invariant Feature Transformation (SIFT). Fitur diekstraksi dari kotak pembatas untuk setiap titik kunci berdasarkan besaran gradien dan orientasi. Ukuran kotak pembatas proporsional dengan skala (yaitu, simpangan baku kernel Gaussian dalam konstruksi ruang skala). Gambar 5.14 menunjukkan titik-titik kunci yang terdeteksi dan kotak-kotak di sekitarnya pada gambar periokular. Sementara fitur GO dan LBP diekstraksi hanya di sekitar mata, fitur SIFT diekstraksi dari semua daerah yang menonjol. Oleh karena itu, pendekatan SIFT diharapkan memberikan lebih banyak kekhasan di antara subjek.



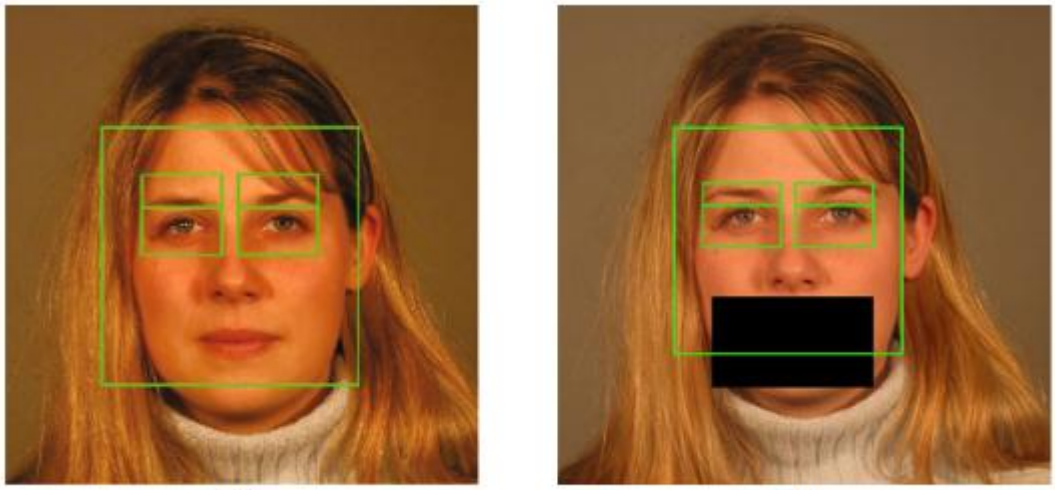
Gambar 5.14 Contoh fitur lokal dan kotak pembatas untuk konstruksi deskriptor menggunakan operator SIFT. **Setiap kotak pembatas diputar sehubungan dengan orientasi atau gradien utama**.

Pencocokan fitur

Untuk fitur GO dan LBP, jarak Euclidean digunakan untuk menghitung skor pencocokan. Skema pencocokan berbasis rasio jarak digunakan untuk SIFT seperti yang dijelaskan di bawah ini.

Diberikan gambar I_i, sekumpulan titik kunci SIFT $K_i = \{K_{i1}, K_{i2}, \ldots, K_{in}\}$ dideteksi. Dalam mencocokkan sepasang gambar I_i dan I_j, semua titik kunci K_i dari I_i dan K_i dari I_j dibandingkan untuk menentukan berapa banyak titik kunci yang berhasil dicocokkan. Jarak Euclidean dari kia ke semua titik kunci di K_j dihitung untuk memperoleh jarak terdekat d_1 dan jarak terdekat kedua d_2. Ketika rasio d_1/d_2 cukup kecil (kurang dari rasio ambang batas), kia dianggap memiliki titik kunci yang cocok di K_j. Dengan menggunakan rasio d_1 dan d_2, baik kesamaan maupun keunikan pasangan titik dipertimbangkan.

Penelitian terkini tentang identifikasi orang menggunakan ciri biometrik periokular, baik dalam spektrum tampak maupun NIR, menunjukkan akurasi identifikasi yang tinggi (lebih dari 80%). Akan tetapi, akurasi tersebut hanya mungkin terjadi jika gambar berkualitas baik dan menunjukkan variasi intra-kelas yang rendah. Telah ditunjukkan pula bahwa biometrik periokular dapat membantu identifikasi orang ketika wajah tertutup. Gambar 5.15 memperlihatkan contoh deteksi wajah dan daerah periokular secara otomatis untuk (a) wajah penuh dan (b) wajah tertutup. Gambar 5.16 memperlihatkan contoh hasil pencocokan citra periokular.

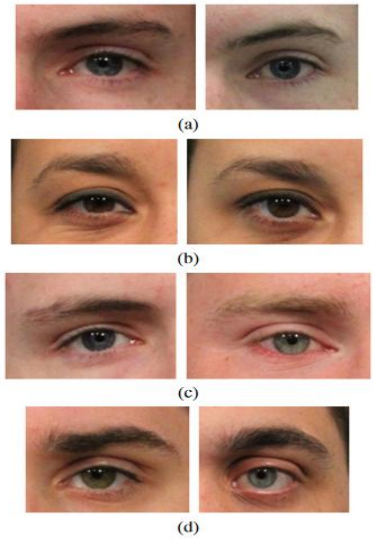


Gambar 5.15 Contoh deteksi wajah dan daerah periokular otomatis pada (a) wajah penuh dan (b) wajah tertutup. Performa pengenalan wajah menurun seiring dengan tertutupnya wajah, tetapi biometrik periokular masih menunjukkan performa identifikasi yang baik. Gambar berasal dari basis data FRGC 2.0.

Tanda wajah

Kemajuan dalam teknologi penginderaan telah mempermudah pengambilan gambar wajah beresolusi tinggi. Dari gambar wajah beresolusi tinggi ini, detail ketidakteraturan kulit, yang juga dikenal sebagai tanda wajah, dapat diekstraksi. Hal ini telah membuka kemungkinan baru dalam representasi wajah dan skema pencocokan. Detail kulit ini sebagian besar diabaikan dan dianggap sebagai gangguan dalam sistem pengenalan wajah yang umum. Namun, tanda wajah dapat digunakan untuk (a) melengkapi pencocok wajah

yang sudah ada guna meningkatkan akurasi identifikasi, (b) memfasilitasi pengambilan citra wajah secara cepat, (c) memungkinkan pencocokan atau pengambilan citra wajah parsial atau off-frontal, dan (d) menyediakan bukti deskriptif lebih lanjut tentang kesamaan atau perbedaan antara citra wajah, yang dapat digunakan sebagai bukti dalam proses hukum. Gambar 5.17 memperlihatkan beberapa jenis tanda wajah yang representatif.



Gambar 5.16 Contoh hasil pencocokan dengan empat pasang gambar periokular yang berbeda dari empat subjek yang berbeda.

Pasangan gambar pada (a) dan (b) berhasil dicocokkan sedangkan pasangan gambar pada (c) dan (d) gagal dicocokkan. Alasan kegagalan adalah karena variasi intra-kelas yang disebabkan oleh perubahan pose dan pencahayaan serta gerakan alis dan kelopak mata.

Praproses

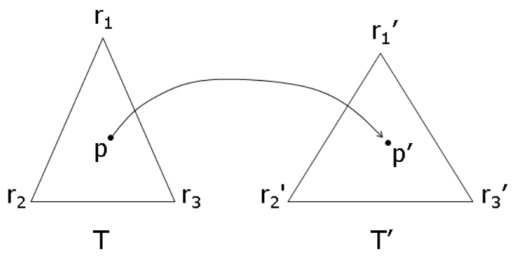
Untuk merepresentasikan tanda wajah dalam sistem koordinat umum, fitur wajah utama seperti mata, alis, hidung, mulut, dan batas wajah (Gambar 5.19) dideteksi dengan menggunakan Model Penampilan Aktif (AAM) atau Model Bentuk Aktif (ASM). Fitur wajah utama ini akan diabaikan dalam proses deteksi tanda wajah berikutnya. Contoh landmark yang dideteksi dalam gambar wajah ditunjukkan pada Gambar 5.19.

Dengan menggunakan landmark yang dideteksi, gambar wajah dipetakan ke bentuk rata-rata untuk menyederhanakan deteksi, pencocokan, dan pengambilan tanda. Misalkan $S_i, i = 1,\ldots,N$ merepresentasikan bentuk masing-masing dari N gambar wajah dalam basis data (galeri) berdasarkan kumpulan landmark. Kemudian, bentuk rata-rata didefinisikan sebagai Sμ = $\sum_{i=1}^{N} S_i$. Setiap gambar wajah, S_i dipetakan ke bentuk rata-rata, S_μ, dengan menggunakan proses pemetaan tekstur berbasis koordinat Barycentric. Pertama, baik S_i maupun S_μ dibagi lagi menjadi sekumpulan segitiga. Diberikan sebuah segitiga T di Si, segitiga yang bersesuaian dengannya T' ditemukan di S_i. Misalkan $r_1 r_2$ dan $r_3(r_1^{'}, r_2^{'}, r_3^{'})$ adalah tiga titik sudut T (T'). Maka, sembarang titik, p, di dalam T dinyatakan sebagai $p = \alpha r_1 + \beta\, r_2 + \gamma r_3$ dan titik yang bersesuaian p' di T' dinyatakan dengan cara yang sama sebagai $p^{'} = a_1^{'} + \beta_2^{'} + \gamma r_3^{'}$, di mana α + β + γ = 1. Dengan cara ini, nilai piksel pada p

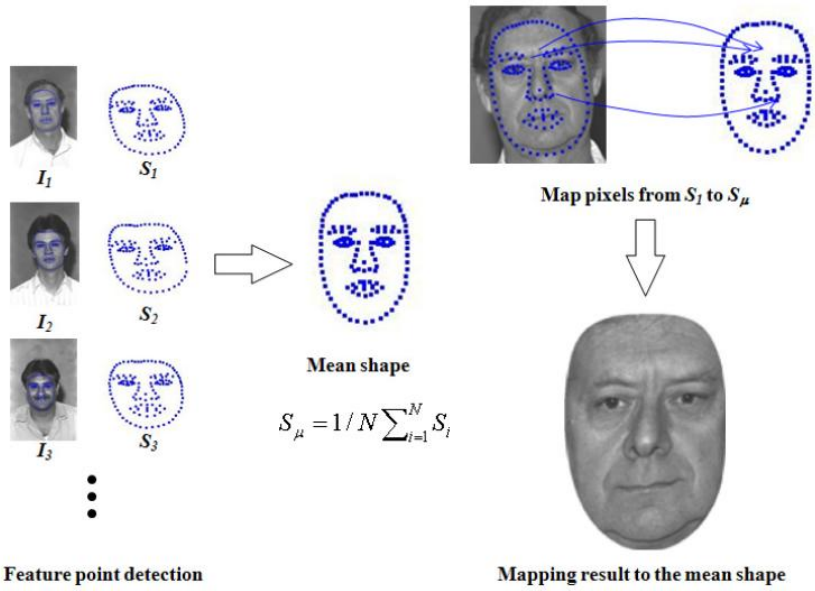
dipetakan ke p'. Gambar 5.18 menunjukkan skema proses pemetaan Barycentric. Dengan mengulang proses pemetaan ini untuk semua titik di dalam semua segitiga, tekstur di S_i dipetakan ke S_μ.

Setelah proses pemetaan ini, semua citra wajah dinormalisasi dalam hal skala dan rotasi dan ini memungkinkan representasi setiap tanda wajah dalam sistem koordinat umum yang berpusat pada wajah. Gambar 5.19 menunjukkan skema konstruksi wajah rata-rata.

Operator deteksi gumpalan diterapkan pada citra wajah yang dipetakan ke dalam bentuk rata-rata. Untuk menekan positif palsu dalam proses deteksi gumpalan yang disebabkan oleh keberadaan fitur wajah primer, masker generik, dilambangkan dengan M_{g}, dibangun dari bentuk rata-rata S_μ. Namun, masker generik tidak mencakup fitur wajah khusus pengguna seperti janggut atau kerutan kecil di sekitar mata atau mulut yang cenderung meningkatkan positif palsu. Oleh karena itu, masker khusus pengguna, M_s, juga dibangun menggunakan citra tepi. Citra tepi diperoleh dengan menggunakan operator Sobel konvensional. Masker khusus pengguna M_{s}, dibuat dengan menjumlahkan M_{g} dan tepian yang terhubung ke M_{g}, membantu menghilangkan sebagian besar positif palsu yang muncul di sekitar jenggot atau kerutan kecil di sekitar mata atau mulut.



Gambar 5.18 Skema proses pemetaan tekstur menggunakan sistem koordinat Barycentric segitiga.



Gambar 5.19 Skema yang menunjukkan konstruksi citra wajah rata-rata.

Deteksi dan klasifikasi tanda

Lindeberg mengusulkan bahwa nilai maksimum lokal pada beberapa skala gambar turunan Gaussian yang dinormalkan (yaitu,$\sigma^2\nabla^2 G$ mencerminkan ukuran karakteristik struktur lokal. Hal ini memungkinkan deteksi gumpalan dengan pemilihan skala otomatis, yang invarian dengan skala gambar. Termotivasi oleh hal ini, kami mendeteksi tanda wajah melalui analisis ruang skala. Deteksi ekstrem ruang skala dimulai dengan membangun representasi multiskala yang dinormalkan dari gambar wajah dengan mengonvolusi gambar input, I(x, y), dengan filter *Laplacian of Gaussian* (LoG) dengan urutan σ_k sebagai

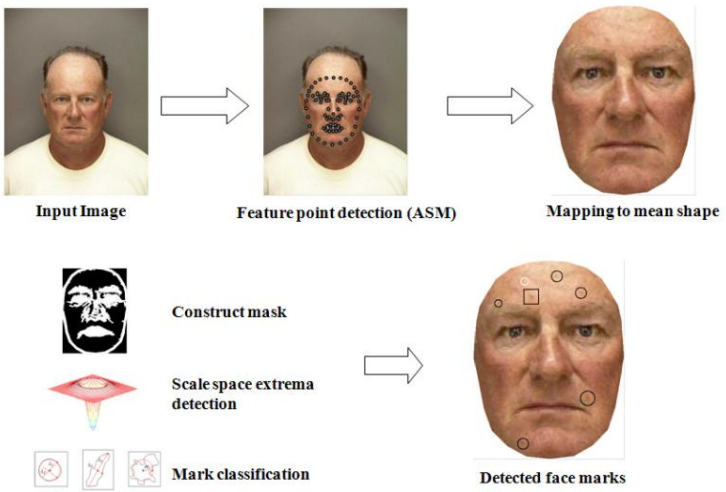
$$\mathrm{D}(\mathrm{x},\mathrm{y},\sigma_k) = \sigma_k^2\nabla^2 G\,(x,y,\sigma_k) * I\,(x,y), k = 1,2,\cdots,n, \qquad (5,6)$$

di mana $\sigma_k^2\nabla^2 G$ adalah operator Laplacian Gaussian yang dinormalisasi skala, dan σ_k = $\mathrm{k}\,\sigma_0, \mathrm{k} = 1,2,\cdots,\mathrm{n}$, dengan σ_0 menjadi nilai konstan $(=\sqrt{2})$ untuk skala awal.

Selanjutnya, ekstrema lokal pada ruang spasial dan skala di setiap blok gambar 3 ×3×3 dideteksi. Lokasi tanda kandidat yang terdeteksi memiliki karakteristik berikut:

- Lokasi yang terdeteksi berisi tanda wajah kandidat.
- Skala yang terdeteksi (σ_k) menunjukkan ukuran tanda wajah yang sesuai.
- Nilai absolut $\mathrm{D}(\mathrm{x},\mathrm{y},\sigma)$ mencerminkan kekuatan respons. Kekuatan ini dapat digunakan sebagai nilai keyakinan untuk memilih tanda yang stabil.
- Tanda $\mathrm{D}(\mathrm{x},\mathrm{y},\sigma)$ membantu dalam menilai intensitas piksel tanda wajah. Tanda positif (negatif) menunjukkan tanda wajah yang gelap (terang) dengan kulit di sekitarnya yang lebih cerah (lebih gelap).

Proses deteksi tanda secara keseluruhan ditunjukkan pada Gambar 5.20.

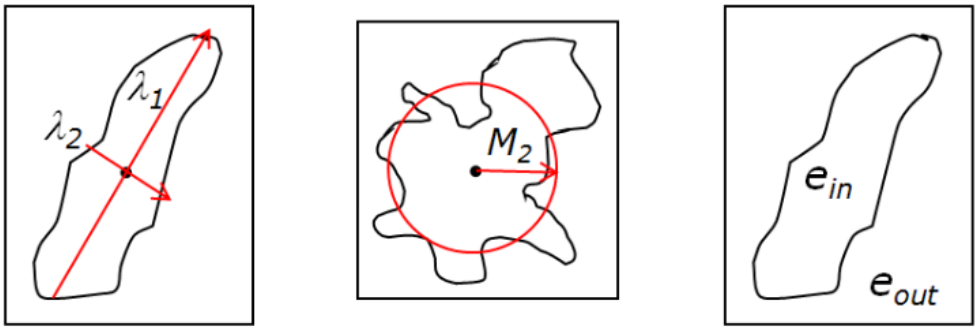


Gambar 5.20 Skema proses deteksi tanda.

Untuk setiap ekstrem lokal yang terdeteksi, kotak pembatas lokal, yang ukurannya proporsional dengan skala terkait, ditentukan. Piksel dalam kotak pembatas dibinerisasi

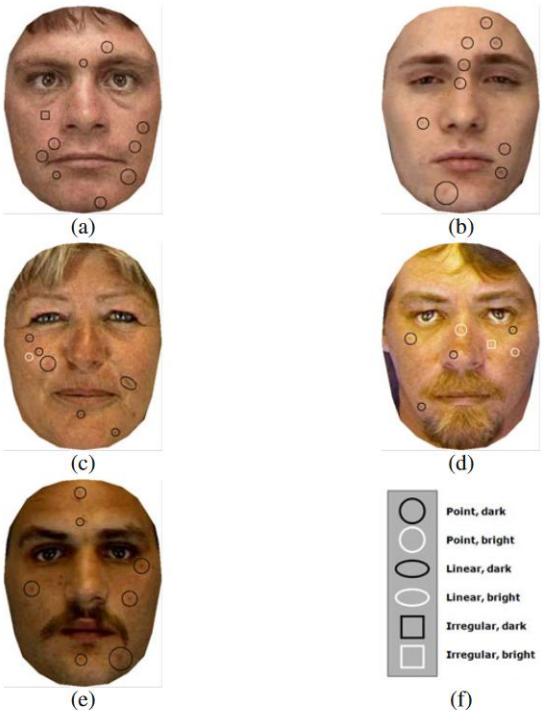
dengan nilai ambang batas yang dipilih sebagai rata-rata piksel di sekitarnya. Ekstrem lokal lebih gelap atau lebih cerah daripada wilayah di sekitarnya, sehingga nilai rata-rata dari area di sekitarnya dapat berfungsi untuk secara efektif menyegmentasikan gumpalan di kotak pembatas. Selanjutnya, gumpalan diklasifikasikan secara hierarkis: 'linier' versus 'semua' diikuti oleh 'melingkar' versus 'tidak teratur'.

Untuk menentukan linearitas, dua nilai eigen λ_1 dan λ_2 diperoleh melalui dekomposisi eigen dari koordinat spasial piksel gumpalan. Ketika λ_1 ecara signifikan lebih besar dari λ_2, tanda tersebut diklasifikasikan sebagai gumpalan linier. Untuk deteksi sirkularitas, pengamatan berikut digunakan: sebuah lingkaran, dengan radius M_2 akan melingkupi sebagian besar piksel gumpalan jika mereka terdistribusi secara melingkar. Oleh karena itu, keputusan 'melingkar' atau 'tidak teratur' dapat dibuat berdasarkan rasio jumlah piksel di dalam dan di luar lingkaran ini. Intensitas piksel gumpalan dapat disimpulkan berdasarkan tanda $\mathrm{D}(\mathrm{x}, \mathrm{y}, \sigma)$, seperti yang dinyatakan sebelumnya. Skema untuk klasifikasi gumpalan ditunjukkan pada Gambar 5.21. Gambar 5.22 mengilustrasikan lima contoh hasil deteksi wajah menggunakan metode deteksi dan klasifikasi tanda yang diusulkan. Dapat diamati bahwa metode yang diusulkan kuat terhadap gangguan dan memberikan perkiraan yang baik tentang ukuran dan kelas tanda.



Gambar 5.21 Skema skema klasifikasi tanda.

Kiri: Nilai eigen λ_1 dan λ_2 dihitung berdasarkan koordinat spasial piksel blob. Dalam contoh ini, nilai eigen terbesar, λ_1 , secara signifikan lebih besar daripada nilai eigen terkecil, λ_2 , sehingga menunjukkan linearitas. Tengah: Sifat melingkar tanda dapat disimpulkan setelah memasang lingkaran pada piksel blob. Di sini, lingkaran dengan radius M_2 digunakan untuk melampirkan piksel di dalam blob. Karena rasio jumlah piksel blob di dalam lingkaran dengan jumlah piksel blob di luar lingkaran besar, tanda ini dapat diberi label sebagai 'melingkar'. Kanan: Tanda perbedaan intensitas piksel antara bagian dalam (e_{in}) dan bagian luar e_{out} blob dapat membantu menilai apakah tanda itu terang atau gelap.

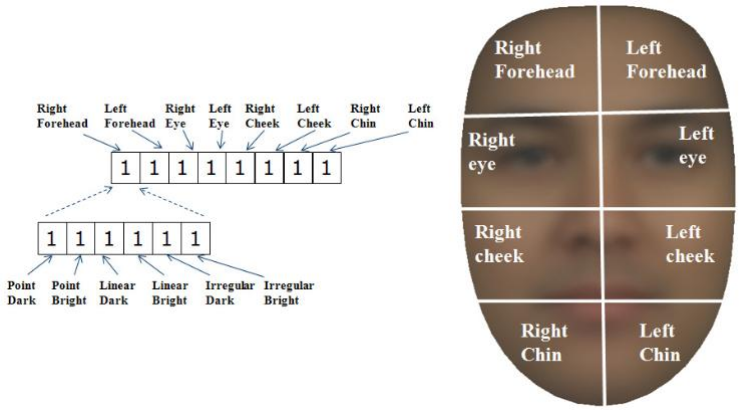


Gambar 5.22 Contoh hasil deteksi dan klasifikasi tanda.

(a), (b), (c), (d), (e) adalah contoh gambar dengan tanda yang terdeteksi. (f) Simbol yang digunakan untuk menunjukkan enam kelas tanda yang berbeda.

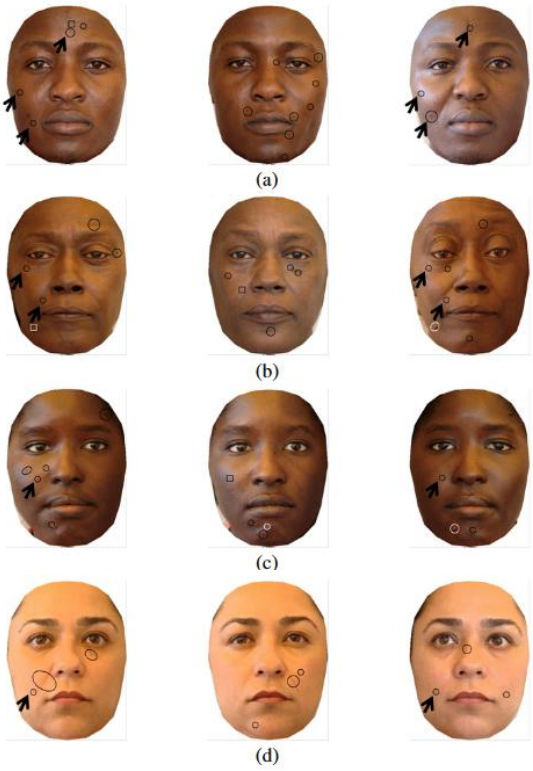
Pencocokan tanda

Tanda wajah yang terdeteksi dikodekan ke dalam histogram 48-bin yang mewakili morfologi, warna, dan lokasi tanda wajah. Untuk mengkodekan informasi lokasi tanda wajah, gambar wajah dalam ruang bentuk rata-rata dibagi lagi menjadi delapan wilayah berbeda seperti yang ditunjukkan pada Gambar 5.23. Setiap tanda dikodekan oleh angka biner enam digit yang mewakili morfologi dan warnanya. Jika ada lebih dari satu tanda di wilayah yang sama, penjumlahan bit demi bit dilakukan. Enam nilai bin digabungkan untuk delapan wilayah berbeda dalam urutan seperti yang ditunjukkan pada Gambar 5.23 untuk menghasilkan histogram 48-bin. Jika suatu tanda diamati pada garis batas segmen wajah, tanda tersebut dimasukkan ke dalam kedua daerah tersebut. Berdasarkan indeks yang diperoleh dari citra wajah, metode perpotongan histogram digunakan untuk menghitung skor pencocokan. Misalkan $H^1(i)$ dan $H^2(j)$ adalah dua histogram yang mewakili indeks tanda, maka perpotongan histogram dihitung sebagai $\sum_{k=1}^{48}(H^1(k)\&H^2(k))$, di mana & mewakili operasi logika dan. Rentang skor pencocokan berdasarkan indeks tanda adalah [0,48].



Gambar 5.23 Skema skema pengindeksan berbasis tanda.

Gambar 5.24 menunjukkan contoh deteksi tanda dan hasil pencocokan dengan basis data saudara kembar identik yang dikumpulkan oleh Universitas Notre Dame. Pada keempat pasang saudara kembar identik yang ditunjukkan dalam gambar ini, tanda wajah membantu membedakan saudara kembar identik jika dikombinasikan dengan mesin pengenalan wajah komersial terkemuka.



Gambar 5.24 Contoh hasil pencocokan dengan empat saudara kembar identik yang berbeda.

Gambar di kolom pertama dan ketiga termasuk subjek yang sama dan gambar di kolom kedua adalah saudara kembar. Kolom pertama, kedua, dan ketiga sesuai dengan probe, pencocokan yang salah hanya menggunakan FaceVACS, dan pasangan sejati yang dicocokkan dengan benar menggunakan FaceVACS dan indeks tanda, masing-masing. Panah hitam di setiap baris menunjukkan tanda wajah yang dideteksi dan diklasifikasikan dengan benar yang berkontribusi untuk mengindividualisasikan saudara kembar identik.

Tato

Penggunaan tato yang dicetak pada tubuh manusia dalam identifikasi tersangka dimulai dengan sistem Bertillon. Sejak saat itu, gambar tato pada tubuh manusia telah dikumpulkan secara rutin dan digunakan oleh lembaga penegak hukum untuk membantu identifikasi tersangka dan korban. Ketika ciri biometrik utama tidak tersedia atau rusak, tato dapat digunakan untuk mengidentifikasi korban atau tersangka.

Gambar 5.25 menunjukkan contoh gambar tato yang digunakan dalam identifikasi korban dan tersangka. Tato memberikan informasi yang lebih diskriminatif daripada indikator demografi tradisional seperti usia, tinggi badan, ras, dan jenis kelamin untuk identifikasi orang. Banyak orang membuat tato untuk menunjukkan kepribadian mereka, atau untuk menunjukkan keanggotaan mereka dalam suatu kelompok. Oleh karena itu, pengenalan tato dapat memberikan pemahaman yang lebih baik tentang latar belakang dan keanggotaan seseorang dalam berbagai organisasi, terutama geng kriminal.

(a) (b)

Gambar 5.25 Contoh gambar tato yang digunakan untuk mengidentifikasi (a) korban Tsunami Asia (2004) di Indonesia dan (b) tersangka.

Gambar 5.26 menunjukkan contoh gambar tato yang menunjukkan keanggotaan dalam geng Mafia Mexikanemi.

(a) (b) (c) (d)

Gambar 5.26 Contoh gambar tato geng yang menunjukkan keanggotaan dalam geng Mafia Mexikanemi di Texas.

Praktik pencocokan tato saat ini didasarkan pada serangkaian kata kunci yang telah ditentukan sebelumnya.

Menetapkan kata kunci ke gambar tato individual membosankan dan subjektif. Sistem pengambilan gambar berbasis konten untuk pengambilan gambar tato dapat mengatasi banyak keterbatasan pengambilan gambar tato berbasis kata kunci. Kami akan menjelaskan secara singkat sistem yang mengekstraksi fitur gambar lokal berdasarkan *Scale Invariant Feature Transform* (SIFT). Informasi kontekstual atau sampingan, yaitu lokasi tato di tubuh dan kata kunci (kelas) yang ditetapkan pada tato, digunakan untuk meningkatkan waktu pengambilan dan akurasi pengambilan. Kendala geometris juga diperkenalkan dalam pencocokan titik kunci SIFT untuk mengurangi pengambilan yang salah.

Kelas tato dan lokasi tubuh

Standar ANSI/NIST-ITL1-2011 mendefinisikan delapan kelas utama (yaitu manusia, hewan, tanaman, bendera, objek, abstrak, simbol, dan lainnya) dan total 70 subkelas (misalnya wajah pria, kucing, narkotika, bendera Amerika, api, sosok, simbol nasional, dan kata-kata) untuk mengkategorikan tato. Pencarian basis data gambar tato melibatkan pencocokan label kelas tato kueri dengan label tato dalam basis data. Prosedur pencocokan tato ini berdasarkan label kelas ANSI/NIST yang ditetapkan secara manual memiliki keterbatasan berikut: (a) label kelas tidak menangkap informasi semantik yang terkandung dalam gambar tato; (b) pemberian label pada jutaan gambar tato yang dikelola oleh lembaga penegak hukum bersifat subjektif dan memakan waktu; (c) tato sering kali berisi beberapa objek dan tidak dapat diklasifikasikan secara memadai ke dalam satu kelas ANSI/NIST; (d) gambar tato memiliki variabilitas intra-kelas yang besar; dan (e) kelas ANSI/NIST tidak lengkap untuk menggambarkan desain tato baru.

Lokasi tato pada tubuh merupakan informasi yang berguna karena dapat diberi tag secara tepat dan objektif. Oleh karena itu, pencarian gambar serupa di lokasi tubuh yang sama dapat secara signifikan mengurangi waktu pencocokan tanpa kehilangan akurasi pencocokan. Pusat Informasi Kejahatan Nasional (NCIC) telah menetapkan 31 kategori utama (misalnya, lengan, betis, dan jari), dan 71 subkategori (misalnya, lengan atas kiri, betis kanan, dan jari tangan kiri) untuk menunjukkan lokasi tato di tubuh.

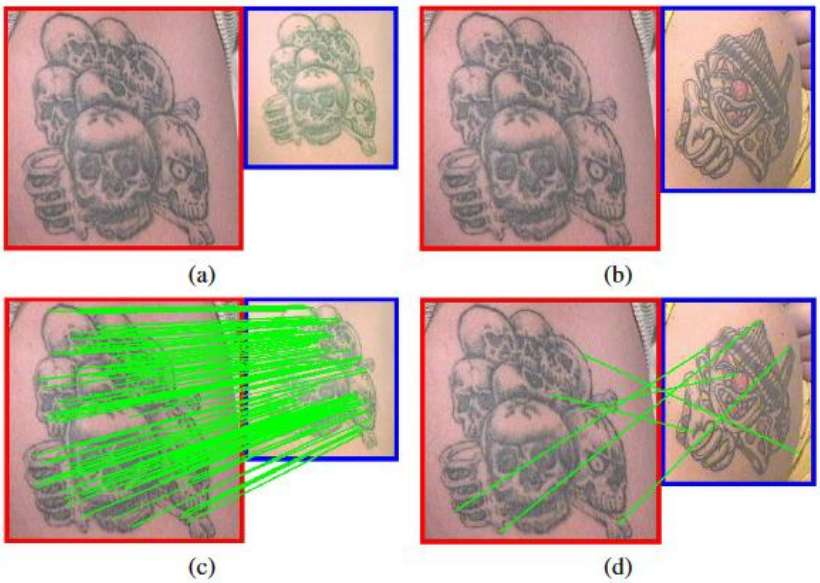
Ekstraksi fitur

Scale Invariant Feature Transform (SIFT) merupakan pendekatan berbasis fitur lokal yang terkenal dan tangguh yang digunakan untuk pengenalan objek. Telah ditunjukkan bahwa fitur SIFT memberikan kinerja yang lebih baik daripada atribut gambar tingkat rendah, (misalnya, warna, tekstur, dan bentuk) untuk pencocokan dan pengambilan gambar tato. SIFT mengekstrak titik fitur karakteristik yang dapat diulang dari gambar dan menghasilkan deskriptor yang mewakili tekstur di sekitar titik fitur. Titik fitur ini invarian terhadap skala dan rotasi gambar, dan terbukti memberikan pencocokan yang tangguh di seluruh rentang distorsi afin, perubahan sudut pandang 3D, noise aditif, dan perubahan pencahayaan.

Pencocokan Fitur

Selain proses pencocokan SIFT konvensional seperti yang dijelaskan di bagian 5.5.1.3, serangkaian kendala geometrik lokal dapat diterapkan untuk mengurangi jumlah titik pencocokan yang salah. Misalkan M_{ij} mewakili serangkaian titik kunci pencocokan antara dua gambar Ii dan Ij. Kemudian, Mij dapat diekspresikan dalam dua himpunan bagian yang berbeda M_{ij} = $M_{ij,T}$ ∪ T $M_{ij,F}$, di mana $M_{ij,T}$ merepresentasikan himpunan titik pencocokan yang benar dan $M_{ij,F}$ merepresentasikan himpunan titik pencocokan yang salah. Diharapkan bahwa menghilangkan titik pencocokan yang salah akan meningkatkan akurasi pengambilan. Jumlah pencocokan yang salah di hadapan variasi sudut pandang atau pengaburan pada gambar cenderung besar.

Ketika titik kunci termasuk dalam $M_{ij,F}$F , titik tersebut cenderung cocok dengan banyak titik kunci lainnya. Di sisi lain, titik kunci dalam $M_{ij,T}$ cenderung cocok dengan satu atau sejumlah kecil titik kunci lainnya. Diberikan gambar kueri I, gambar tersebut dicocokkan dengan semua gambar dalam basis data galeri D dan jumlah titik pencocokan diperoleh untuk setiap gambar galeri. Biarkan $L_m, m = 1, 2, 3, \ldots$, merepresentasikan himpunan titik kunci dalam gambar kueri yang dicocokkan ke dalam titik kunci yang sama di D. Biarkan ukuran area yang dicakup oleh Lm menjadi Am. Kemudian, Lm dianggap sebagai milik $M_{ij,F}$ jika Am lebih besar dari ambang batas t $(t = 0{,}2)$. Semua titik kunci yang cocok yang tidak ada di $M_{ij,F}$ dianggap sebagai titik pencocokan yang sebenarnya. Terakhir, jumlah titik kunci yang termasuk dalam $M_{ij,T}$ digunakan untuk mengambil gambar kandidat N teratas dari basis data gambar tato. Gambar 5.27 menunjukkan contoh hasil pencocokan pada pasangan gambar tato duplikat dan non-duplikat. Jumlah titik kunci yang cocok untuk pasangan duplikat diamati jauh lebih besar daripada pasangan non-duplikat.



Gambar 5.27 Contoh pencocokan tato.

Sepasang gambar tato (a) duplikat dan (b) non-duplikat dan hasil pencocokan SIFT-nya. Ada 129 dan 12 titik kunci yang cocok pada pasangan (c) duplikat dan (d) non-duplikat, masing-masing. Jumlah oktaf dan skala dipilih masing-masing 3 dan 4. Vektor fitur yang dikaitkan dengan setiap titik kunci memiliki 128 dimensi.

Gambar 5.28 menunjukkan contoh hasil pencarian gambar tato berdasarkan pencocok SIFT, lokasi tubuh, dan label kelas ANSI/NIST untuk tiga kueri yang berbeda. Untuk kueri 1, tiga gambar duplikat yang berbeda dari basis data berhasil diambil pada peringkat 1, 2, dan 6. Skor pencocokan yang sesuai untuk ketiga gambar yang diambil ini adalah: 163, 157, dan 26. Skor rendah untuk gambar ketiga yang diambil pada peringkat 6 mungkin disebabkan oleh kontras rendah (memudar) tato. Dua tato duplikat diambil, pada peringkat 1 dan 2, untuk kueri 2 dan satu gambar duplikat diambil untuk kueri 3 pada peringkat 6. Perlu dicatat bahwa karena ukuran tato pada kueri 3 kecil, jumlah titik kunci SIFT yang diekstraksi kecil dan karenanya semua skor kecocokan untuk gambar yang diambil juga rendah.

Gambar 5.28 Contoh pengambilan. Setiap baris menunjukkan kueri dan 7 gambar teratas yang diambil beserta skor kecocokan terkait.

Ringkasan

Berbagai macam ciri biometrik telah dipelajari dalam literatur. Mengingat semakin berkembangnya domain aplikasi biometrik, kemungkinan penggunaan ciri biometrik lunak seperti telinga, gaya berjalan, geometri tangan, dan biometrik lunak akan menjadi lazim dan juga diperlukan dalam beberapa konteks. Hal ini akan memungkinkan perancangan sistem biometrik yang efektif yang memanfaatkan rangkaian ciri biometrik yang paling tepat berdasarkan faktor-faktor seperti skenario aplikasi, sifat populasi target, ketersediaan ciri biometrik, sumber daya komputasi yang tersedia, dll. Dengan demikian, menyelidiki modalitas biometrik baru untuk penggunaan potensial terutama dalam skenario pengguna yang tidak dibatasi dan tidak kooperatif memiliki manfaatnya sendiri.

Pada saat yang sama, seseorang perlu menetapkan kekhasan ciri biometrik, keawetannya, dan kerentanannya terhadap pemalsuan. Namun, ini bisa menjadi latihan yang agak membosankan dan berbelit-belit. Misalnya, meskipun pencocokan sidik jari telah digunakan selama lebih dari 100 tahun dalam forensik, keunikan atau individualitas sidik jari masih menjadi bidang penelitian yang sedang berlangsung. Demikian pula, pemodelan proses penuaan wajah dan pengaruhnya terhadap akurasi pencocokan wajah merupakan

bidang penelitian yang aktif. Dalam kasus iris, tidak ada data longitudinal untuk mulai menyelidiki fenomena penuaan. Jadi, saat ciri-ciri biometrik baru dipelajari, tanggung jawab berada pada peneliti untuk menganalisis kelebihan dan kekurangan setiap ciri dan menentukan nilai tambahnya.

BAB 6
MULTIBIOMETRIK

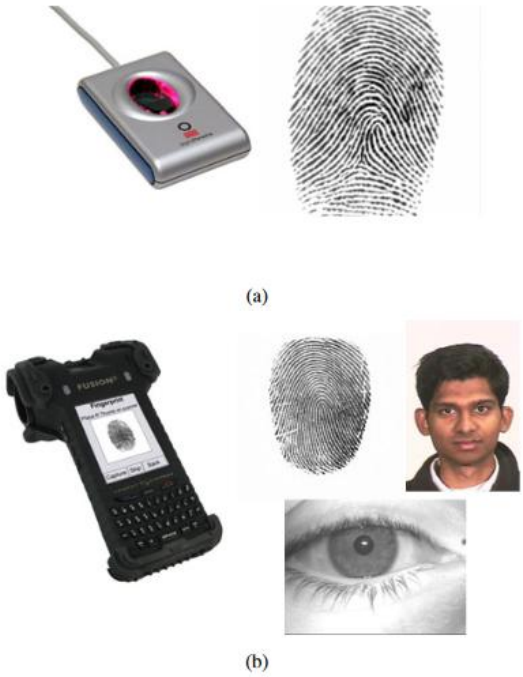
Sistem pengenalan orang yang menggabungkan bukti dari berbagai sumber informasi biometrik untuk menentukan identitas seseorang dikenal sebagai sistem multibiometrik. Misalnya, ciri wajah dan iris, atau sidik jari dari kesepuluh jari seseorang, dapat digunakan bersama-sama untuk menentukan identitas orang tersebut secara akurat dan kuat. Sistem multibiometrik dapat mengatasi banyak keterbatasan sistem unibiometrik karena sumber biometrik yang berbeda biasanya saling mengimbangi keterbatasan yang melekat satu sama lain.

Oleh karena itu, sistem multibiometrik umumnya diharapkan lebih andal dan akurat daripada sistem unibiometrik, serta menyediakan cakupan populasi yang lebih luas (mengurangi tingkat kegagalan pendaftaran). Proses konsolidasi informasi atau bukti yang disajikan oleh berbagai sumber biometrik dikenal sebagai fusi informasi, yang merupakan fokus utama bab ini. Lebih khusus lagi, bab ini memperkenalkan berbagai sumber dan jenis informasi biometrik yang dapat digabungkan dan berbagai metodologi penggabungan.

6.1 PENDAHULUAN

Sistem pengenalan orang berdasarkan ciri biometrik individu seperti sidik jari, wajah, dan iris telah menjadi fokus buku ini sejauh ini. Sebagian besar sistem biometrik ini dapat diberi label sebagai sistem unibiometrik karena mengandalkan satu sumber biometrik tunggal untuk pengenalan. Setiap bukti yang dapat digunakan secara independen untuk mengenali seseorang disebut sumber informasi biometrik. Sistem unibiometrik memiliki beberapa keterbatasan. Bagaimana jika sumber biometrik menjadi tidak dapat diandalkan karena sensor atau perangkat lunak tidak berfungsi dengan baik, kualitas buruk dari ciri biometrik spesifik pengguna, atau manipulasi yang disengaja?

Lebih jauh lagi, aplikasi keamanan tinggi dan sistem identifikasi sipil skala besar memberlakukan persyaratan akurasi yang ketat yang tidak dapat dipenuhi oleh sistem unibiometrik yang ada. Contoh aplikasi tersebut termasuk program US-VISIT dan sistem Identifikasi Unik (UID) di India, di mana identitas sejumlah besar individu (ratusan juta) perlu dipecahkan. Untuk memenuhi persyaratan aplikasi tersebut, ada kebutuhan untuk bergerak melampaui paradigma tradisional pengenalan biometrik berdasarkan satu sumber informasi biometrik dan mempertimbangkan sistem yang menggabungkan bukti dari berbagai sumber biometrik untuk pengenalan.



Gambar 6.1 Ilustrasi Sistem Unibiometrik Dan Multibiometrik.

Sistem unibiometrik mengenali pengguna berdasarkan satu sumber biometrik tunggal misalnya, satu cetakan sidik jari yang diambil menggunakan sensor sidik jari, sistem multibiometrik mengidentifikasi pengguna berdasarkan beberapa sumber biometrik; sistem multibiometrik Fusion yang dikembangkan oleh Cogent Systems, yang mampu mengambil gambar sidik jari, wajah, dan iris mata seseorang ditunjukkan pada gambar (b). Manusia mengenali satu sama lain berdasarkan bukti yang disajikan oleh beberapa karakteristik biometrik (misalnya, wajah, gaya berjalan, dan suara) di samping detail kontekstual (misalnya, pengetahuan sebelumnya tentang keberadaan seseorang pada waktu dan lokasi tertentu).

Proses pengenalan itu sendiri dapat dilihat sebagai rekonsiliasi bukti yang berkaitan dengan beberapa sumber informasi ini. Setiap sumber sendiri tidak selalu dapat digunakan secara andal untuk melakukan pengenalan. Namun, konsolidasi informasi yang disajikan oleh berbagai isyarat ini dapat menghasilkan penentuan atau verifikasi identitas yang lebih akurat. Demikian pula, sistem biometrik juga dapat dirancang untuk mengenali seseorang berdasarkan informasi yang diperoleh dari berbagai sumber biometrik. Sistem semacam itu, yang dikenal sebagai sistem multibiometrik, diharapkan lebih akurat dibandingkan dengan sistem unibiometrik yang mengandalkan satu bukti biometrik. Sistem multibiometrik bukanlah hal baru. Faktanya, sistem biometrik pertama yang dikembangkan oleh Bertillon (lihat Bab 1), dapat dianggap sebagai sistem multibiometrik karena menggabungkan bukti dari berbagai pengukuran tubuh manusia. Demikian pula, Sistem Identifikasi Sidik Jari Otomatis (AFIS) yang digunakan oleh lembaga penegak hukum di seluruh dunia secara rutin menangkap kesepuluh jari dan kemudian menggabungkan keputusan yang dibuat

berdasarkan jari-jari individu untuk mendapatkan keputusan identitas yang lebih andal pada subjek.

Peningkatan akurasi, yang merupakan motivasi utama untuk menggunakan sistem multibiometrik, terjadi karena dua alasan. Pertama, penggabungan beberapa sumber biometrik secara efektif meningkatkan dimensionalitas ruang fitur dan mengurangi tumpang tindih antara distribusi fitur individu yang berbeda. Dengan kata lain, kombinasi beberapa sumber biometrik lebih unik bagi satu individu daripada sampel biometrik tunggal. Kedua, gangguan, ketidaktepatan, atau penyimpangan inheren (yang disebabkan oleh faktor-faktor seperti penuaan) dalam sebagian sumber biometrik dapat dikompensasi oleh informasi diskriminatif yang disediakan oleh sumber yang tersisa. Dengan demikian, ketersediaan beberapa sumber biometrik memberikan redundansi dan toleransi kesalahan dalam arti bahwa sistem pengenalan terus beroperasi bahkan ketika modul akuisisi biometrik tertentu gagal. Selain meningkatkan akurasi pengenalan, sistem multibiometrik juga dapat menawarkan keuntungan dibandingkan sistem unibiometrik seperti:

1. Mengurangi masalah non-universalitas dan mengurangi kegagalan untuk mendaftarkan kesalahan. Misalnya, jika seseorang tidak dapat didaftarkan dalam sistem sidik jari karena detail tonjolannya sudah usang atau jari-jarinya hilang , ia masih dapat diidentifikasi menggunakan ciri-ciri lainnya seperti wajah atau iris mata.
2. Memberikan fleksibilitas dalam autentikasi pengguna. Misalkan seorang pengguna mendaftar ke dalam sistem menggunakan beberapa ciri yang berbeda. Kemudian, pada saat autentikasi, hanya sebagian kecil dari ciri-ciri ini yang dapat diperoleh berdasarkan sifat aplikasi yang dipertimbangkan dan kenyamanan pengguna. Sistem multibiometrik juga dapat membantu dalam pemantauan atau pelacakan berkelanjutan terhadap seorang individu dalam situasi ketika satu ciri saja tidak mencukupi atau tidak tersedia setiap saat.
3. Memungkinkan pencarian basis data biometrik yang besar dengan cara yang efisien secara komputasi. Hal ini dapat dicapai dengan terlebih dahulu menggunakan modalitas yang relatif sederhana tetapi kurang akurat untuk memangkas basis data sebelum menggunakan modalitas yang lebih kompleks dan akurat pada data yang tersisa untuk melakukan tugas identifikasi akhir, sehingga meningkatkan hasil dari sistem identifikasi biometrik.
4. Meningkatkan ketahanan terhadap serangan spoof. Hal ini karena semakin sulit untuk menghindari beberapa sumber biometrik secara bersamaan. Lebih jauh lagi, dengan meminta pengguna untuk menyajikan subset ciri acak pada titik akuisisi, sistem multibiometrik dapat memfasilitasi mekanisme tantangan-respons yang memverifikasi keberadaan pengguna yang masih hidup. Sebagai contoh, seseorang dapat didaftarkan dengan kesepuluh sidik jari, tetapi pada saat autentikasi, sistem dapat memintanya untuk menyajikan hanya tiga jari dalam urutan tertentu (telunjuk kiri, diikuti oleh telunjuk kanan, diikuti oleh jari tengah kiri).

Meskipun sistem multibiometrik menawarkan sejumlah keuntungan, sistem ini biasanya lebih mahal daripada sistem unibiometrik karena memerlukan perangkat keras tambahan

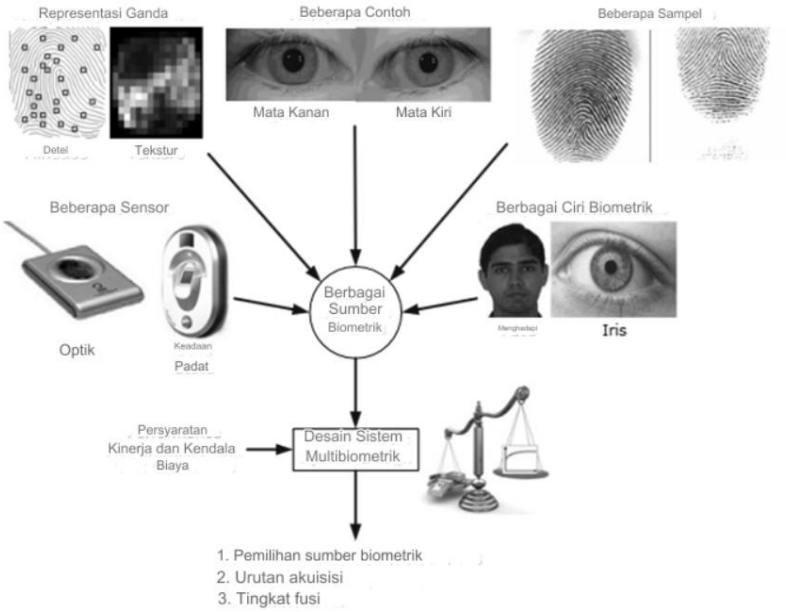
(sumber daya komputasi atau penyimpanan) dan waktu pendaftaran serta pengenalan yang lebih lama. Oleh karena itu, penting untuk menganalisis dengan cermat tradeoff antara biaya tambahan dan manfaat yang diperoleh saat membuat kasus bisnis untuk penggunaan multibiometrik dalam aplikasi tertentu. Meskipun memiliki keterbatasan ini, sistem multibiometrik semakin banyak digunakan dalam banyak sistem identifikasi skala besar yang melibatkan jutaan pengguna misalnya, sistem kontrol perbatasan atau identitas nasional karena kemampuannya untuk mencapai akurasi pengenalan yang tinggi berdasarkan teknologi yang ada, yang jauh lebih besar daripada biaya tambahan dalam aplikasi tersebut. Dalam merancang sistem multibiometrik, kita perlu mengatasi empat masalah desain berikut:

1. Sumber informasi: Apa saja berbagai sumber informasi biometrik yang harus digunakan dalam sistem multibiometrik?
2. Modus operasi: Haruskah data yang berkaitan dengan beberapa sumber biometrik diperoleh secara bersamaan dalam modus paralel atau berurutan? Demikian pula, haruskah informasi yang diperoleh diproses secara berurutan atau bersamaan?
3. Tingkat penggabungan: Jenis informasi apa (misalnya, data mentah, fitur, skor kecocokan, atau keputusan) yang akan digabungkan?
4. Pendekatan penggabungan: Skema penggabungan apa yang harus digunakan untuk menggabungkan informasi yang disajikan oleh beberapa sumber biometrik?

Bagian selanjutnya mempertimbangkan masing-masing pertanyaan ini secara bergantian. Namun, perlu diingat bahwa pertanyaan-pertanyaan ini tidak sepenuhnya independen. Misalnya, pilihan sumber biometrik dapat menentukan strategi akuisisi atau jenis informasi yang akan digabungkan.

6.2 SUMBER BERBAGAI BUKTI

Ada lima kemungkinan skenario yang dapat menyediakan berbagai sumber informasi biometrik seperti yang ditunjukkan pada Gambar 6.2. Berdasarkan sumber bukti, sistem multibiometrik dapat diklasifikasikan menjadi sistem multisensor, multialgoritma, multiinstansi, multisampel, dan multimodal. Dalam empat skenario pertama, beberapa bukti berasal dari satu ciri biometrik misalnya, sidik jari atau iris, sedangkan dalam skenario kelima (sistem biometrik multimodal) beberapa ciri biometrik misalnya, sidik jari dan iris)digunakan. Sistem multibiometrik juga memungkinkan untuk memanfaatkan kombinasi dua atau lebih dari lima skenario yang dibahas di bawah ini. Misalnya, karena sistem UID di India menggunakan kesepuluh jari dan dua iris, sistem tersebut bersifat multiinstansi dan multimodal. Sistem seperti itu disebut sistem multibiometrik hibrida.



Gambar 6.2 Sistem Multibiometrik Memanfaatkan Informasi Dari Berbagai Sumber Biometrik Untuk Menetapkan Identitas.

Berdasarkan sumber informasi yang digunakan, sistem multibiometrik dapat diklasifikasikan menjadi sistem multisensor, multialgoritma, multiinstansi, multisampel, dan multimoda. Dalam empat skenario pertama, satu ciri biometrik menyediakan berbagai sumber bukti. Dalam skenario kelima, berbagai ciri biometrik digunakan sebagai sumber bukti. Meskipun pada prinsipnya, sejumlah besar sumber dapat digabungkan untuk meningkatkan akurasi identifikasi, faktor praktis seperti biaya penyebaran, ukuran sampel pelatihan yang kecil, persyaratan akurasi, waktu pemrosesan, dan penerimaan pengguna akan membatasi jumlah sumber yang digunakan dalam aplikasi tertentu.

Sistem multisensor

Dalam sistem ini, satu ciri biometrik dicitrakan atau ditangkap menggunakan berbagai sensor untuk mengekstrak informasi yang beragam. Misalnya, suatu sistem dapat merekam konten tekstur dua dimensi wajah seseorang menggunakan kamera CCD dan bentuk permukaan tiga dimensi (citra kedalaman atau jangkauan) wajah menggunakan sensor jangkauan untuk melakukan autentikasi. Pengenalan sensor baru atau sensor jangkauan untuk mengukur variasi permukaan wajah meningkatkan biaya sistem multibiometrik.

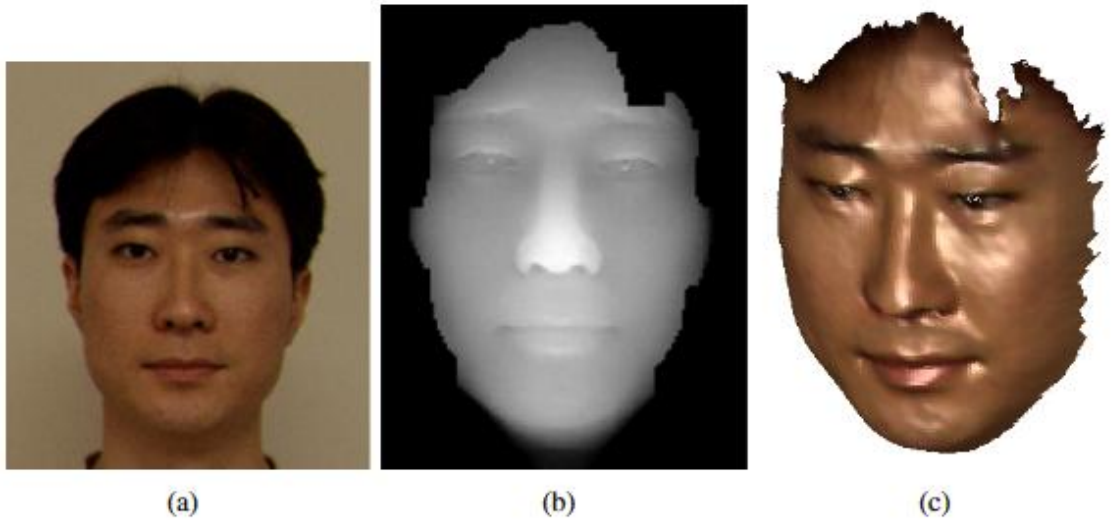
Namun, ketersediaan data multisensor yang berkaitan dengan satu sifat tidak hanya dapat meningkatkan akurasi pencocokan sistem pengenalan secara keseluruhan, tetapi juga membantu dalam tahap pemrosesan antara dari masing-masing sistem komponen seperti segmentasi dan registrasi gambar.

Tabel 6.1 Ketergantungan Antara Pilihan Desain Dalam Sistem Multibiometrik.

Sumber Multi-biometrik	Jenis Informasi Yang Digabungkan	Arsitektur Akuisisi	Arsitektur Pemrosesan

	Data Mentah	Fitur	Skor
Beberapa Sensor	✓	✓	✓
Beberapa Representasi	×	✓	✓
Beberapa Matcher	×	×	✓
Beberapa Instance	×	✓	✓
Beberapa Sampel	✓	✓	✓
Beberapa Sifat	×	✓	✓

Tanda centang (✓) menunjukkan bahwa kedua pilihan desain tersebut kompatibel, sedangkan tanda silang (×) menunjukkan bahwa kedua pilihan tersebut tidak kompatibel.



Gambar 6.3 Membangun Tekstur Wajah 3D Dengan Menggabungkan Bukti Yang Disajikan Oleh Gambar Tekstur 2D Dan Gambar Rentang 3D.

a).Tekstur wajah 2D seseorang, b) Gambar rentang 3D atau kedalaman yang sesuai (di sini, biru menunjukkan jarak yang lebih jauh dari kamera sedangkan merah menunjukkan jarak yang lebih dekat), c) Permukaan 3D setelah memetakan informasi tekstur 2D dari (a).

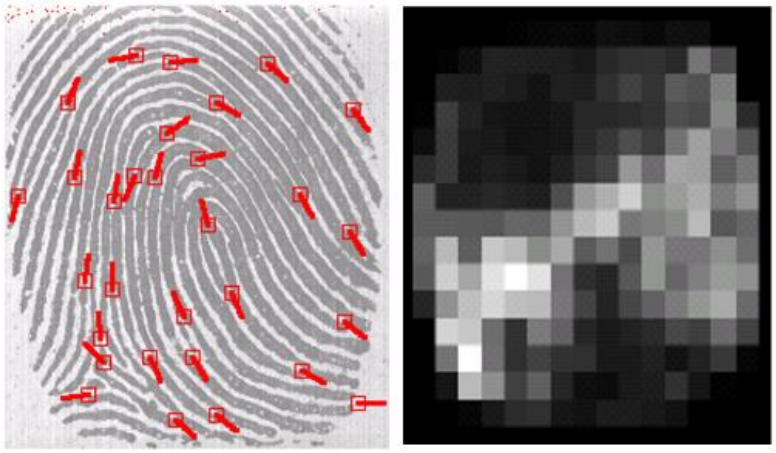
Contoh lain dari fusi multisensor adalah penggunaan kamera inframerah termal dan kamera cahaya tampak untuk pengenalan wajah. Registrasi spasial antara data yang diperoleh dari beberapa sensor biasanya merupakan salah satu masalah mendasar dalam merancang sistem multisensor. Namun, hal ini mungkin tidak selalu terjadi dan ada sistem multisensor di mana registrasi sudah tertanam pada sensor atau registrasi mungkin tidak diperlukan.

Sensor jangkauan yang memperoleh gambar tekstur 2D dan gambar jangkauan 3D pada Gambar 6.3 adalah contoh dari kategori pertama. Jika sensor sidik jari optik dan kapasitif digunakan untuk menangkap sidik jari, kedua gambar sidik jari dapat diproses secara independen tanpa mendaftarkannya secara spasial. Namun, dalam skenario ini, pengguna diharuskan untuk berinteraksi dengan sensor satu per satu, yang menyebabkan waktu pendaftaran dan verifikasi yang lebih lama.

Sistem multialgoritma

Dalam sistem ini, data biometrik yang sama diproses menggunakan beberapa algoritma. Misalnya, algoritma berbasis tekstur dan algoritma berbasis minutiae dapat beroperasi pada gambar sidik jari yang sama untuk mengekstrak berbagai set fitur yang dapat meningkatkan kinerja sistem. Sistem semacam ini tidak memerlukan penggunaan sensor baru dan, karenanya, hemat biaya. Lebih jauh lagi, karena pengguna tidak diharuskan berinteraksi dengan beberapa sensor, tidak ada ketidaknyamanan tambahan. Namun, hal itu memerlukan pengenalan modul ekstraktor dan/atau pencocok fitur baru, yang dapat meningkatkan persyaratan komputasi sistem.

Keterbatasan utama sistem multi-algoritma adalah karena sumber bukti yang berbeda diperoleh dari data mentah yang sama (misalnya, gambar sidik jari telunjuk kanan), berbagai sumber cenderung berkorelasi. Ini biasanya membatasi kemungkinan peningkatan akurasi pencocokan. Misalnya, jika citra sidik jari yang diperoleh berisik, hal itu akan memengaruhi algoritme berbasis tekstur dan berbasis minutiae, tetapi pada tingkat yang berbeda.



Gambar 6.4 Ekstraksi Kumpulan Fitur Yang Berbeda Dari Citra Sidik Jari Yang Sama.

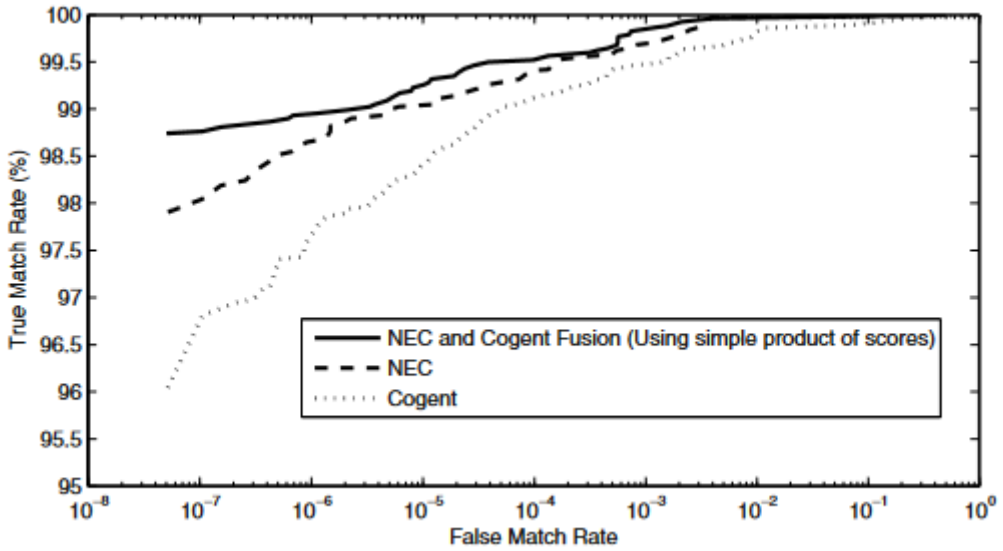
a. Fitur minutia yang diekstraksi dari citra sidik jari

b. fitur tekstur yang diekstraksi dari citra sidik jari pada (a).

Contoh ini diambil dari Fingerprint Vendor Technology Evaluation (FpVTE) yang dilakukan oleh National Institute of Standards and Technology (NIST) pada tahun 2003. Penggabungan bukti dari dua pencocok paling akurat dalam FpVTE 2003, yaitu NEC dan Cogent Systems, menghasilkan peningkatan marjinal dalam True Accept Rate (juga dikenal sebagai Genuine Accept Rate) dibandingkan dengan pencocok individu.

Gambar 6.5 menunjukkan contoh di mana penggabungan beberapa algoritme meningkatkan akurasi. Sistem multi-algoritma dapat menggunakan beberapa set fitur (yaitu, beberapa representasi) yang diekstrak dari data biometrik yang sama atau beberapa skema pencocokan yang beroperasi pada satu set fitur. Kombinasi algoritme berbasis tekstur dan algoritme pencocokan sidik jari berbasis minutiae (ditunjukkan pada Gambar 6.4) adalah

contoh dari kategori pertama, sementara penggabungan hasil dari beberapa pencocok minutiae seperti transformasi Hough, pencocokan string satu dimensi, dan pemrograman dinamis dua dimensi adalah ilustrasi dari yang terakhir.



Gambar 6.5 Peningkatan Akurasi Dalam Sistem Verifikasi Sidik Jari Multi-Algoritma.

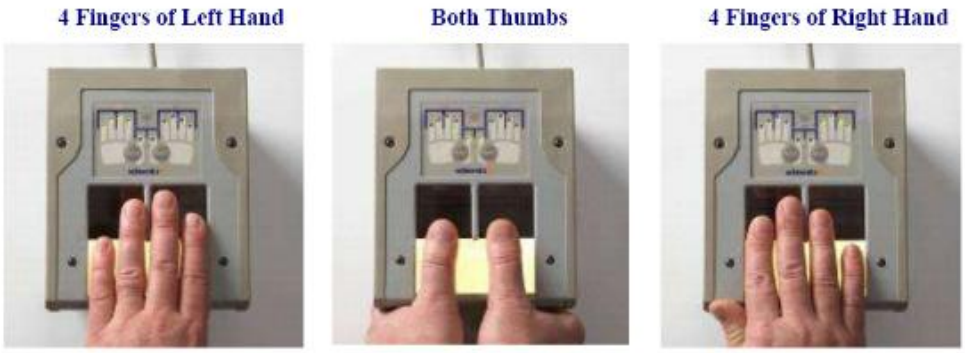
Contoh lain dari sistem yang menggunakan beberapa set fitur adalah sistem pengenalan wajah yang menggunakan skema ekstraksi fitur berbeda seperti Analisis Komponen Utama (PCA), Analisis Komponen Independen (ICA), dan Analisis Diskriminan Linear (LDA) untuk mengodekan (yaitu, mewakili) gambar wajah tunggal.

Sistem multi-instansi

Sistem ini menggunakan beberapa instans dari ciri tubuh yang sama dan terkadang disebut juga sebagai sistem multi-unit. Misalnya, jari telunjuk kiri dan kanan, atau iris mata kiri dan kanan seseorang dapat digunakan untuk memverifikasi identitas seseorang. Sistem ini umumnya tidak memerlukan pengenalan sensor baru atau memerlukan pengembangan algoritma ekstraksi dan pencocokan fitur baru dan, oleh karena itu, lebih mudah diimplementasikan. Namun, dalam beberapa kasus, pengaturan sensor baru mungkin diperlukan untuk memfasilitasi penangkapan berbagai unit/instansi secara bersamaan. Sistem Identifikasi Sidik Jari Otomatis (AFIS), yang memperoleh informasi sepuluh sidik jari dari subjek, dapat memperoleh manfaat dari sensor yang mampu memperoleh kesan sepuluh jari dengan cepat dalam tiga tahap seperti yang ditunjukkan pada Gambar 6.6.

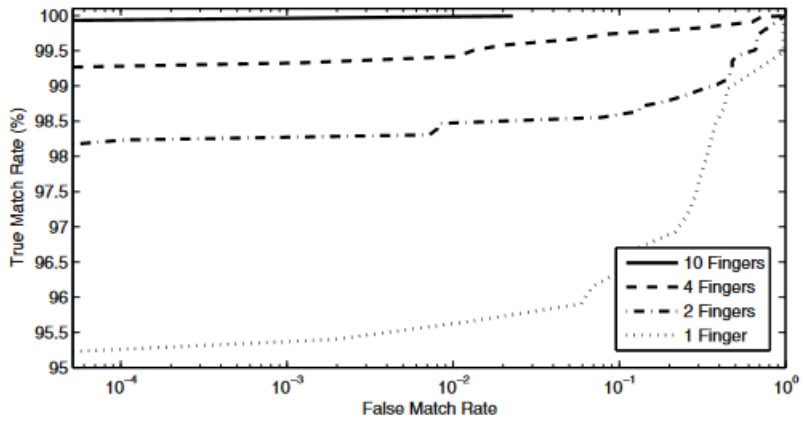
Sistem multi-instansi sangat bermanfaat bagi pengguna yang ciri biometriknya tidak dapat ditangkap dengan andal karena masalah yang melekat. Misalnya, satu jari mungkin bukan pembeda yang memadai bagi seseorang dengan kulit jari kering. Namun, integrasi bukti di beberapa jari dapat berfungsi sebagai pembeda yang baik dalam kasus ini. Demikian pula, sistem iris mungkin tidak dapat mencitrakan bagian penting dari iris seseorang karena kelopak mata yang terkulai. Pertimbangan kedua iris akan menghasilkan ketersediaan

informasi tekstur tambahan yang dapat digunakan untuk menetapkan identitas individu secara andal.



Gambar 6.6 Sensor Sidik Jari Yang Dikembangkan Oleh Identix Yang Memungkinkan Akuisisi Cepat Kesepuluh Jari Dalam Tiga Langkah. (Sumber: Nationwide Solutions)

Sistem multi-instansi sering kali diperlukan dalam aplikasi yang ukuran basis data sistemnya (yaitu, jumlah individu yang terdaftar) sangat besar (basis data IAFIS FBI saat ini memiliki lebih dari 60 juta gambar sepuluh sidik jari) dan kesepuluh sidik jari tersebut memberikan informasi diskriminatif tambahan yang diperlukan untuk akurasi pencarian yang tinggi (lihat Gambar 6.7). Karena alasan ini, Departemen Keamanan Dalam Negeri (DHS) di Amerika Serikat, yang awalnya hanya mengumpulkan dua jari telunjuk untuk program kontrol perbatasan US-VISIT, sekarang mengumpulkan kesepuluh sidik jari tersebut.



Gambar 6.7 Peningkatan akurasi dalam sistem verifikasi sidik jari multi-instansi. Contoh yang diekstrak dari FpVTE 2003 ini menunjukkan bahwa penggabungan bukti dari beberapa jari menghasilkan peningkatan signifikan dalam akurasi.

Sistem multi-sampel

Sensor tunggal dapat digunakan untuk memperoleh beberapa sampel dari ciri biometrik yang sama untuk memperhitungkan variasi yang dapat terjadi pada ciri tersebut, atau untuk memperoleh representasi yang lebih lengkap dari ciri yang mendasarinya. Sistem

wajah, misalnya, dapat menangkap dan menyimpan gambar profil kiri dan kanan bersama dengan gambar frontal wajah seseorang untuk memperhitungkan variasi dalam pose wajah.

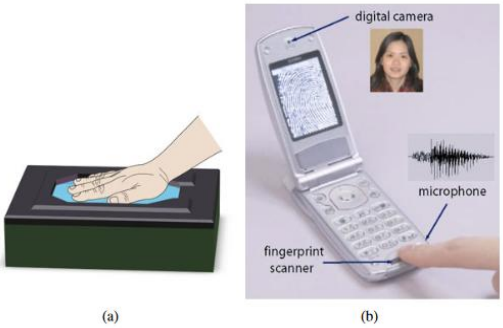
Demikian pula, sistem sidik jari yang dilengkapi dengan sensor dengan area penginderaan kecil dapat memperoleh beberapa sidik jari dari jari seseorang untuk menangkap berbagai area sidik jari. Citra sidik jari ini dapat digabungkan untuk membentuk sidik jari yang lengkap, yang akan memberikan sejumlah besar detail. Salah satu masalah utama dalam sistem multi-sampel adalah menentukan jumlah sampel yang perlu diperoleh dari sifat biometrik. Penting bahwa sampel yang diperoleh mewakili variabilitas serta kekhasan data biometrik individu.

Untuk mencapai tujuan ini, protokol pengumpulan sampel yang tepat yang memperhitungkan variabilitas sampel harus ditetapkan sebelumnya. Misalnya, sistem pengenalan wajah yang memanfaatkan citra profil depan dan samping1 dari seorang individu dapat menetapkan bahwa citra profil samping harus berupa tampilan tiga perempat wajah. Sebagai alternatif, dengan serangkaian sampel biometrik, sistem harus dapat secara otomatis memilih subset optimal yang paling baik mewakili variabilitas individu.

Sistem multimoda

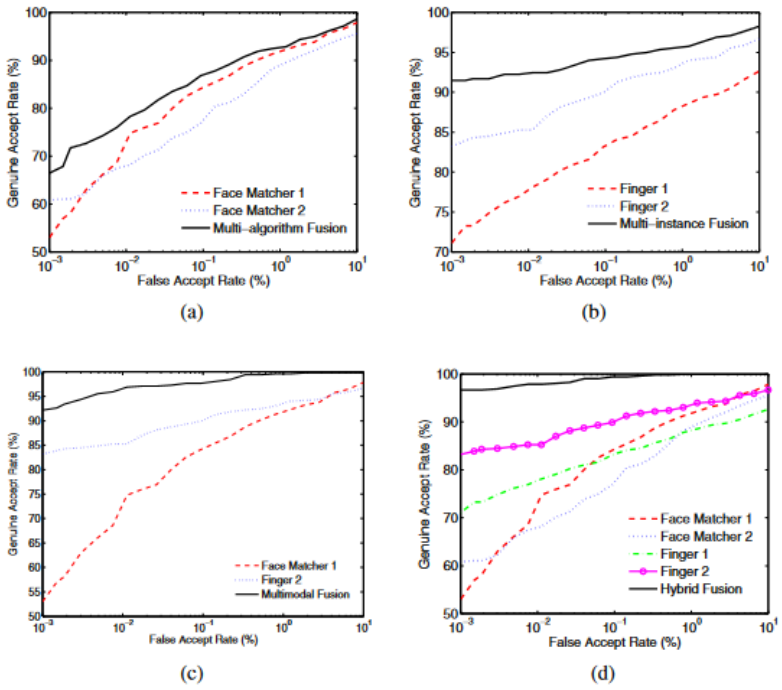
Sistem multimoda menggabungkan bukti yang disajikan oleh berbagai ciri tubuh untuk menetapkan identitas. Beberapa sistem biometrik multimoda paling awal menggunakan fitur wajah dan suara untuk menetapkan identitas seseorang. Karena berbagai ciri biometrik seseorang diharapkan tidak berkorelasi misalnya, sidik jari dan iris, penggunaan sistem biometrik multimoda umumnya menghasilkan peningkatan kinerja yang lebih besar dibandingkan dengan jenis sistem multibiometrik lainnya. Namun, beberapa kombinasi ciri biometrik misalnya, suara dan gerakan bibir dapat menunjukkan korelasi yang signifikan, dan penggunaan kombinasi tersebut mungkin tidak memberikan peningkatan kinerja yang signifikan.

Biaya penerapan sistem biometrik multimoda jauh lebih besar karena persyaratan beberapa sensor dan, akibatnya, pengembangan antarmuka pengguna yang. Meskipun akurasi identifikasi dapat ditingkatkan secara signifikan dengan memanfaatkan semakin banyak ciri, jumlah ini umumnya dibatasi oleh pertimbangan praktis seperti biaya penyebaran, waktu pendaftaran, throughput, tingkat kesalahan yang diharapkan, masalah pembiasaan pengguna, dll. Lebih jauh lagi, ada hasil yang semakin berkurang setelah ciri biometrik yang kuat (misalnya, sidik jari dan iris) telah digabungkan. Bahkan, tergantung pada skema penggabungan, mungkin ada penurunan kinerja jika banyak ciri biometrik dengan akurasi yang lebih rendah ditambahkan.



Gambar 6.8 Contoh Antarmuka Yang Dapat Merekam Data Multibiometrik.

a. *Diagram konsep pemindai seluruh tangan yang dapat secara bersamaan memperoleh sidik telapak tangan, sidik jari dari kelima jari tangan, dan bentuk tanga*
b. *Telepon seluler yang dapat memperoleh beberapa modalitas seperti sidik jari, wajah, dan suara. Upaya awal juga telah dilakukan untuk memodifikasi kamera pada telepon untuk menangkap citra iris mata juga.*



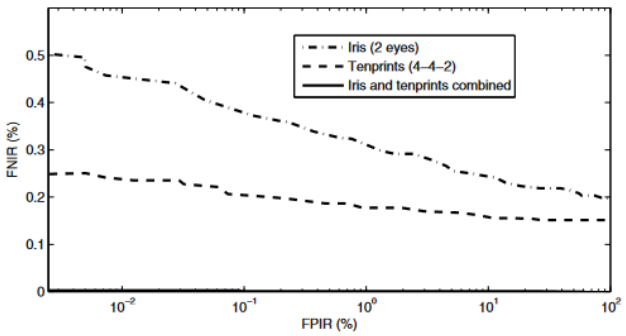
Gambar 6.9 Perbandingan Peningkatan Akurasi Dalam Berbagai Jenis Sistem Multibiometrik Berdasarkan Basis Data NIST-Biometric Score Set Release 1 (BSSR1).

a. *Sistem multi-algoritma, di mana bukti digabungkan dari dua pencocok wajah berbeda yang beroperasi pada citra wajah yang sama*
b. *sistem multi-instansi, di mana informasi dari dua jari berbeda digabungkan, dan (c) sistem multimoda, di mana bukti diakumulasikan dari satu jari dan wajah. (d) Sistem multibiometrik hibrida, di mana sumber informasi mencakup dua jari dan dua pencocok wajah.*

Meskipun kelima jenis sistem multibiometrik yang disebutkan di atas memiliki kelebihan dan kekurangannya sendiri, sistem biometrik multi-instance dan multimodal lebih populer daripada tiga jenis lainnya, karena mereka menawarkan cakupan yang lebih besar untuk meningkatkan akurasi pengenalan dan meningkatkan cakupan populasi. Banyak sistem identifikasi biometrik skala besar yang digunakan dalam aplikasi praktis termasuk FBI-

IAFIS, US-VISIT, dan proyek *Unique Identification* (UID) di India menggunakan beberapa instance atau beberapa ciri atau kombinasi keduanya.

Selain lima skenario di atas, juga memungkinkan untuk menggunakan ciri-ciri biometrik bersama dengan autentikator non-biometrik seperti token atau kata sandi. Ketika lebih dari satu faktor identifikasi (di antara kata sandi, token, dan ciri-ciri biometrik) digunakan, skenario tersebut disebut sebagai autentikasi multi-faktor.



Gambar 6.10 Peningkatan Akurasi Dalam Sistem Identifikasi Biometrik Multi-Instansi Dan Multimoda Dengan Modalitas Sidik Jari Dan Iris (Sumber: Otoritas UID India).

Perhatikan bahwa dalam aplikasi seperti UID, tempat deduplikasi ratusan juta identitas perlu dilakukan, diperlukan Tingkat Identifikasi Positif Palsu (FPIR) yang sangat rendah serta Tingkat Identifikasi Negatif Palsu (FNIR) yang sangat rendah. Tingkat akurasi ini dapat dicapai hanya jika kesepuluh jari dan kedua iris digabungkan. Perhatikan bahwa penggabungan 10 sidik jari dan 2 iris pada basis data 20.000 subjek ini menghasilkan FNIR dan FPIR yang hampir nol.

6.3 ARSITEKTUR AKUISISI DAN PEMROSESAN

Salah satu pertimbangan utama saat merancang sistem biometrik adalah kegunaannya. Penting untuk merancang antarmuka pengguna yang ergonomis dan nyaman, yang dapat secara efisien menangkap citra biometrik berkualitas baik, yang mengarah pada tingkat kegagalan pendaftaran yang lebih rendah. Hal ini khususnya berlaku dalam kasus sistem multibiometrik, karena beberapa bukti yang berkaitan dengan identitas individu harus diperoleh dengan andal sambil menyebabkan ketidaknyamanan minimum bagi pengguna.

Urutan atau sekuens akuisisi data biometrik memiliki pengaruh pada kenyamanan yang diberikan kepada pengguna. Lebih jauh, urutan pemrosesan data biometrik yang diperoleh dapat secara signifikan memengaruhi waktu pemrosesan dalam sistem identifikasi skala besar (melibatkan jutaan pengguna terdaftar) karena keputusan identifikasi dapat dibuat dengan cepat dengan jumlah ciri yang relatif kecil.

Urutan akuisisi

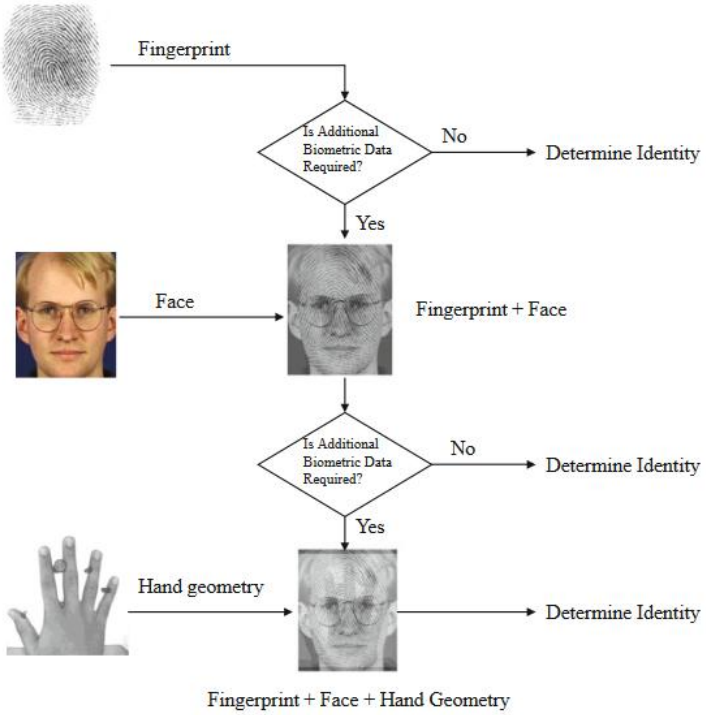
Urutan akuisisi dalam sistem multibiometrik mengacu pada urutan perolehan berbagai sumber bukti dari individu (dalam kasus sistem multi-algoritma, hanya diperlukan

satu sampel biometrik dan, oleh karena itu, metodologi akuisisi tidak menjadi masalah). Urutan akuisisi bisa berupa serial atau paralel. Biasanya, sistem multibiometrik menggunakan pendekatan akuisisi serial, di mana bukti dikumpulkan secara berurutan, yaitu, setiap sumber diperoleh secara independen dengan interval waktu yang singkat antara akuisisi yang berurutan. Dalam beberapa kasus, bukti dapat diperoleh secara bersamaan secara paralel.

Misalnya, informasi wajah dan iris pengguna dapat diperoleh hampir bersamaan dengan memanfaatkan dua kamera yang ditempatkan di unit yang sama. Demikian pula, wajah, suara, dan gerakan bibir pengguna dapat diperoleh secara bersamaan dengan merekam video, dan beberapa sidik jari dapat diambil secara paralel menggunakan pemindai multi-jari. Sementara akuisisi serial tidak memerlukan pengaturan sensor khusus dan biasanya memiliki biaya pemasangan yang lebih rendah, akuisisi paralel dapat mengurangi waktu pendaftaran dan autentikasi serta meningkatkan kegunaan sistem multibiometrik.

Urutan pemrosesan

Urutan pemrosesan yang diadopsi oleh sistem multibiometrik mengacu pada urutan pemrosesan informasi yang diperoleh untuk menghasilkan keputusan yang dapat terlepas dari urutan perolehan informasi. Dengan demikian, informasi dapat diperoleh secara berurutan tetapi diproses secara bersamaan dan sebaliknya.

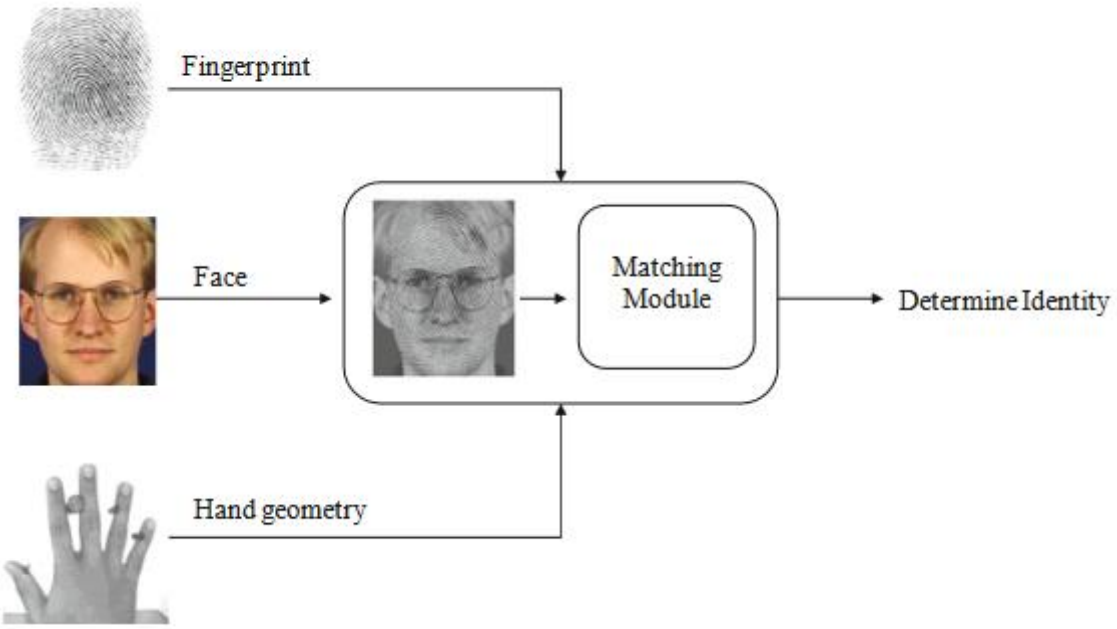


Gambar 6.11 Dalam Mode Operasi Bertingkat (Atau Serial), Bukti Diproses Secara Bertahap Untuk Menetapkan Identitas Pengguna.

Skema ini juga dikenal sebagai pengenalan pola berurutan. Skema ini meningkatkan kenyamanan pengguna sekaligus mengurangi waktu pemrosesan rata-rata karena keputusan dapat dibuat tanpa harus memperoleh semua ciri biometrik. Dalam mode serial atau

kaskade, pemrosesan informasi berlangsung secara berurutan. Pada Gambar 6.11, informasi sidik jari pengguna diproses terlebih dahulu; jika subsistem sidik jari tidak dapat menentukan identitas pengguna, maka data yang sesuai dengan biometrik wajah diproses. Dalam pengaturan seperti itu, waktu pemrosesan dapat dikurangi secara efektif jika keputusan dibuat tanpa menunggu keluaran dari semua sistem unibiometrik.

Pengguna juga dapat diizinkan untuk memilih ciri biometrik mana yang harus diambil terlebih dahulu, yang menghasilkan kemudahan yang lebih besar. Selain meningkatkan kenyamanan pengguna, skema berjenjang juga memungkinkan pencarian cepat dan efisien dalam tugas identifikasi skala besar (juga disebut pengindeksan atau penyaringan basis data). Hasil pencocokan yang diperoleh menggunakan setiap modalitas dapat digunakan untuk memangkas basis data secara berurutan, sehingga membuat pencarian lebih cepat dan lebih efisien. Namun, algoritme yang kuat sangat penting untuk menangani secara efisien berbagai rangkaian kejadian yang mungkin terjadi dalam sistem multibiometrik berjenjang.



Gambar 6.12 Dalam Mode Operasi Paralel, Bukti Yang Diperoleh Dari Beberapa Sumber Diproses Secara Bersamaan Untuk Menetapkan Identitas Pengguna.

Perhatikan bahwa bukti yang berkaitan dengan beberapa sumber dapat diperoleh secara berurutan. Dalam mode paralel, setiap sistem unibiometrik memproses informasinya secara independen pada saat yang sama dan informasi yang diproses digabungkan menggunakan skema fusi yang sesuai. Sistem multibiometrik yang dirancang untuk beroperasi dalam mode paralel umumnya memiliki akurasi yang lebih tinggi karena menggunakan lebih banyak bukti tentang pengguna untuk pengenalan.

Sebagian besar sistem multibiometrik praktis memiliki arsitektur paralel karena tujuan utama perancang sistem multibiometrik adalah untuk mengurangi tingkat kesalahan

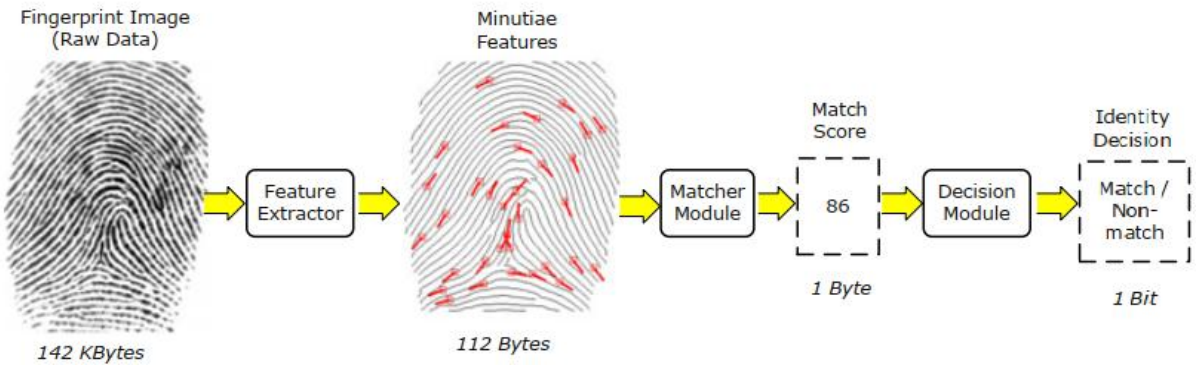
sistem biometrik dan tidak harus mengurangi throughput dan/atau waktu pemrosesan. Namun, keputusan tentang jumlah sumber biometrik optimal yang akan digunakan masih perlu dibuat dan mungkin melibatkan studi tentang keseimbangan antara akurasi dan faktor lain seperti biaya sistem dan hasil.

Selain dua mode operasi yang dibahas di atas, arsitektur hierarkis (seperti pohon) juga dapat digunakan untuk menggabungkan keunggulan arsitektur bertingkat dan paralel. Dalam skema semacam itu, sebagian dari modalitas yang diperoleh dapat digabungkan secara paralel, sementara modalitas yang tersisa dapat digabungkan secara serial. Arsitektur semacam itu dapat ditentukan secara dinamis berdasarkan kualitas sampel biometrik individual serta saat menemukan data biometrik yang hilang.

6.4 TINGKAT PENGGABUNGAN

Masalah mendasar dalam desain sistem multibiometrik adalah menentukan jenis informasi yang harus dikonsolidasikan oleh modul penggabungan. Dalam sistem biometrik yang umum, jumlah informasi yang tersedia untuk sistem akan dikompresi saat seseorang berpindah dari modul sensor ke modul keputusan. Data biometrik mentah misalnya, gambar atau video adalah yang paling kaya akan konten informasi dan pemrosesan selanjutnya misalnya, ekstraksi fitur mengurangi jumlah informasi yang tersedia untuk sistem. Namun, perlu dicatat bahwa penggunaan representasi tingkat fitur untuk penggabungan memiliki beberapa keuntungan dibandingkan representasi tingkat sensor yaitu, tingkat data mentah.

Pertama, ekstraksi fitur diharapkan dapat memberikan representasi invarian dari pola biometrik yang sedang dipertimbangkan. Kedua, efek noise diharapkan akan berkurang setelah ekstraksi fitur, yang biasanya melibatkan operasi peningkatan untuk menekan noise inheren dalam data biometrik. Namun, prosedur peningkatan itu sendiri dapat menambahkan beberapa informasi palsu ke data mentah asli. Dengan demikian, terdapat interaksi antara jumlah informasi bermanfaat yang tersedia pada setiap tahap dalam sistem biometrik dan tingkat gangguan yang merusak informasi ini.



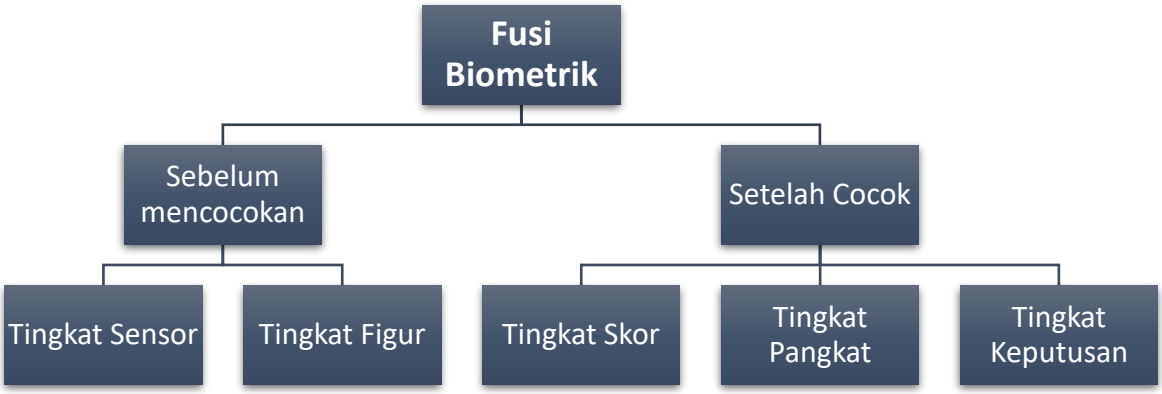
Gambar 6.13 Jumlah Informasi Yang Tersedia Untuk Fusi Berkurang Saat Seseorang Maju Melalui Berbagai Modul Pemrosesan Sistem Biometrik.

Data mentah merupakan sumber informasi terkaya, sementara keputusan akhir (dalam skenario verifikasi) hanya berisi sedikit informasi. Namun, data mentah tersebut rusak

karena gangguan dan mungkin memiliki variabilitas intra-kelas yang besar, yang biasanya berkurang dalam modul sistem berikutnya. Dalam sistem multibiometrik, fusi dapat dilakukan dengan memanfaatkan informasi yang tersedia di salah satu dari empat modul biometrik yakni sensor, ekstraktor fitur, pencocok, dan modul keputusan.

Gambar 6.14 menunjukkan berbagai tingkat fusi yang mungkin dalam sistem multibiometrik. Fusi biometrik dapat secara luas diklasifikasikan menjadi (a) fusi sebelum pencocokan, dan (b) fusi setelah pencocokan. Perbedaan ini dibuat karena setelah pencocok dipanggil, jumlah informasi yang tersedia untuk sistem fusi berkurang drastis. Selain itu, fusi sebelum pencocokan dapat diterapkan selama pendaftaran dan/atau autentikasi. Di sisi lain, fusi setelah pencocokan hanya dapat diterapkan selama autentikasi.

Sebelum pencocokan, integrasi informasi dari berbagai sumber biometrik dapat dilakukan baik pada tingkat sensor maupun pada tingkat fitur. Skema untuk integrasi informasi setelah tahap klasifikasi/pencocokan dapat dibagi lagi menjadi tiga kategori: penggabungan pada tingkat keputusan, penggabungan pada tingkat peringkat, dan penggabungan pada tingkat skor pencocokan.



Gambar 6.14 Penggabungan Dapat Dilakukan Pada Berbagai Tingkatan Dalam Sistem Biometrik.

Sebagian besar sistem multibiometrik menggabungkan informasi pada tingkat skor atau tingkat keputusan. Penggabungan pada tingkat peringkat hanya berlaku untuk sistem biometrik yang beroperasi dalam mode identifikasi. Sistem biometrik yang mengintegrasikan informasi pada tahap awal pemrosesan diyakini lebih efektif daripada sistem yang melakukan integrasi pada tahap selanjutnya. Karena rangkaian fitur berisi informasi yang lebih kaya tentang pola biometrik masukan daripada skor kecocokan atau label keputusan, integrasi pada tingkat fitur diharapkan memberikan hasil pengenalan yang lebih baik daripada penggabungan tingkat skor atau keputusan.

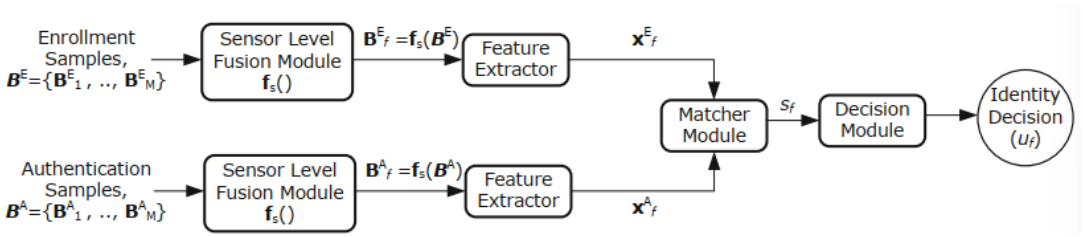
Namun, dalam praktiknya hal ini tidak selalu benar karena (a) proses fusi harus memperhitungkan keberadaan noise dalam set fitur penyusun, dan (b) algoritme pencocokan baru mungkin diperlukan untuk membandingkan dua set fitur yang digabungkan. Mengembangkan algoritme pencocokan yang efisien sering kali merupakan

aspek yang paling menantang dalam desain sistem biometrik dan, dengan demikian, fusi pada level sensor atau fitur menimbulkan kompleksitas pemrosesan tambahan.

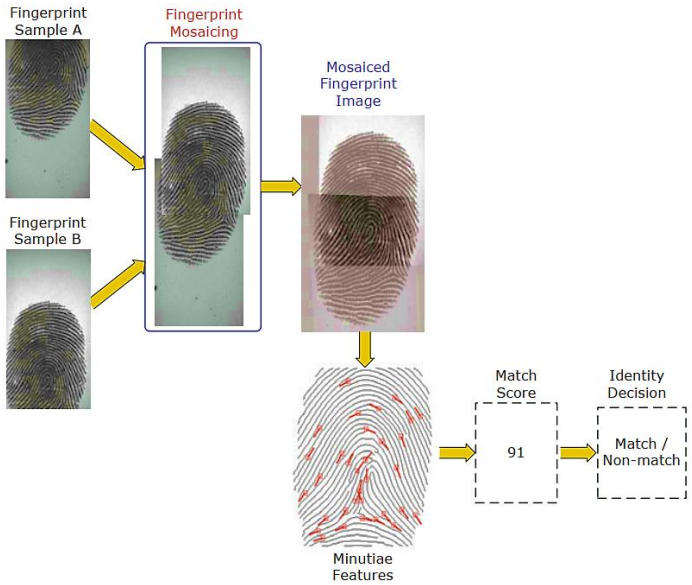
Fusi level sensor

Fusi level sensor memerlukan konsolidasi bukti yang disajikan oleh beberapa sumber data mentah sebelum data tersebut diekstraksi fiturnya. Dalam literatur pemrosesan gambar, hal ini disebut sebagai fusi level gambar atau level piksel. Frasa "fusi level sensor" digunakan untuk mengakomodasi jenis data mentah lainnya seperti suara, video, dll. Aliran informasi dalam sistem multibiometrik yang menggunakan fusi level sensor ditunjukkan pada Gambar 6.15. Sementara Gambar 6.15 menunjukkan bahwa fusi tingkat sensor dilakukan selama pendaftaran dan autentikasi, hal ini tidak selalu terjadi. Dimungkinkan untuk merancang sistem multibiometrik di mana fusi hanya diterapkan selama pendaftaran atau selama autentikasi. Secara umum, fungsi fusi tingkat sensor $\mathbf{f}_s(.)$ mengubah kumpulan sampel biometrik M adalah $\mathbf{B} = \{\mathbf{B}_1, \mathbf{B}_2.., \mathbf{B}_M\}$ menjadi sampel tunggal yang difusikan $\mathbf{B}_f$, yaitu,

$$\mathbf{B}_f = \mathbf{f}_s\{\mathbf{B}_1, \mathbf{B}_2.., \mathbf{B}_M\} \tag{6.1}$$



Gambar 6.15 Aliran Informasi Dalam Sistem Multibiometrik Yang Menggunakan Fusi Tingkat Sensor.



Gambar 6.16 Ilustrasi Skema Fusi Tingkat Sensor Di Mana Beberapa Cetakan Jari Yang Sama Dijahit Bersama Menggunakan Proses Yang Disebut Mosaik Untuk Menghasilkan Citra Sidik Jari Komposit.

Fusi tingkat sensor hanya berlaku untuk sistem multisensor dan multisampel. Misalnya, sensor sidik jari kecil dapat menangkap dua atau lebih cetakan sidik jari seseorang dan membuat citra sidik jari komposit yang memperlihatkan struktur tonjolan yang lebih lengkap (lihat Gambar 6.16). Proses ini, yang dikenal sebagai mosaik, khususnya berguna dalam sensor sapuan di mana setiap irisan gambar hanya mewakili sebagian kecil sidik jari dan, oleh karena itu, diperlukan algoritma penjahitan yang tepat untuk mengintegrasikan berbagai irisan guna membentuk citra sidik jari yang lengkap.

Penjahitan mosaik juga dapat dilakukan dalam pengenalan wajah di mana beberapa citra 2D yang mewakili berbagai pose dapat dijahit untuk menghasilkan satu citra. Dimungkinkan juga untuk menggabungkan tekstur 2D wajah seseorang dengan pemindaian 3D yang sesuai (misalnya, citra rentang) untuk membuat model tekstur 3D. Ketersediaan model ini memungkinkan pembuatan citra 2D wajah seseorang yang baru (yang sebelumnya tidak terlihat) (misalnya, pada berbagai pose, pencahayaan, kemiringan kepala, dll.) tanpa benar-benar menggunakan pemindai untuk menangkap citra tersebut.

Penggabungan tingkat fitur

Penggabungan tingkat fitur atau representasi melibatkan konsolidasi bukti yang disajikan oleh dua set fitur biometrik berbeda dari individu yang sama. Gambar 6.17 menunjukkan aliran informasi umum dalam sistem multibiometrik menggunakan penggabungan tingkat fitur. Secara matematis, fungsi penggabungan tingkat fitur $\mathbf{f}_R(.)$ mengubah kumpulan M set fitur biometrik $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M\}$ menjadi satu set fitur gabungan $\mathbf{x}_f$, yaitu,

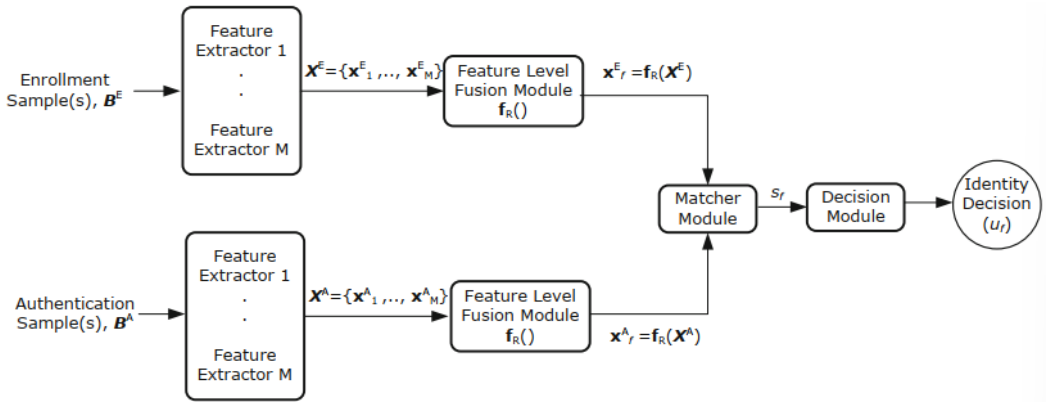
$$\mathbf{x}_f = \mathbf{f}_R(\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M) \tag{6.2}$$

Skema fusi tingkat fitur dapat dikategorikan ke dalam dua kelas besar, yaitu homogen dan heterogen. Skema fusi fitur homogen digunakan ketika set fitur yang akan digabungkan diperoleh dengan menerapkan algoritma ekstraksi fitur yang sama ke beberapa sampel dari sifat biometrik yang sama (misalnya, set minu-tia dari dua cetakan jari yang sama). Pendekatan ini berlaku untuk sistem multi-sampel dan multi-sensor. Teknik fusi fitur heterogen diperlukan jika set fitur komponen berasal dari algoritma ekstraksi fitur yang berbeda atau dari sampel sifat biometrik yang berbeda atau contoh yang berbeda dari sifat yang sama.

Fusi fitur homogen

Fusi fitur homogen dapat digunakan untuk pembaruan templat atau perbaikan templat seperti yang dibahas di bawah ini. ***Pembaruan templat***: Templat dalam basis data dapat diperbarui berdasarkan bukti yang disajikan oleh set fitur saat ini untuk mencerminkan (mungkin) perubahan permanen dalam biometrik seseorang. Sistem geometri tangan menggunakan proses ini untuk memperbarui pengukuran geometris yang disimpan dalam basis data untuk memperhitungkan perubahan pada tangan seseorang selama periode waktu tertentu. Biasanya, templat diperbarui setelah setiap autentikasi berhasil. Oleh karena itu, aliran informasi dalam sistem seperti itu tidak mengikuti aliran umum yang ditunjukkan

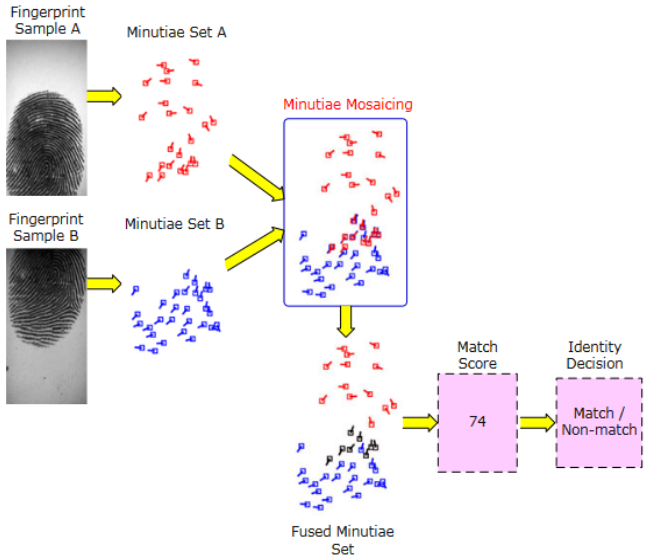
pada Gambar 6.17. Di sini, rata-rata templat saat ini (x^E) dan vektor fitur baru yang diperoleh selama autentikasi (x^A) dihitung dan disimpan sebagai templat baru (x^E), asalkan autentikasi berhasil.



Gambar 6.17 Alur Informasi Umum Dalam Sistem Multibiometrik Yang Menggunakan Fusi Tingkat Fitur.

$$\hat{X}^E \begin{cases} \dfrac{X^E + X^A}{2}, \text{jika } \mathcal{M}(X^E, X^A) \geq \tau \\ X^E, \qquad\qquad \text{jika tidak,} \end{cases} \tag{6.3}$$

di mana $\mathcal{M}$ adalah fungsi pencocokan yang menghitung kesamaan antara dua vektor fitur dan τ adalah ambang batas keputusan. ***Peningkatan templat***: Dalam kasus sidik jari, informasi minutiae yang tersedia dalam dua cetakan dapat digabungkan dengan menyelaraskan kedua cetakan dengan tepat dan kemudian menghilangkan minutiae duplikat, sehingga menghasilkan set minutiae yang lebih besar.



Gambar 6.18 Ilustrasi Skema Fusi Fitur Homogen (Perbaikan Templat) Di Mana Kumpulan Minutia Yang Diekstraksi Dari Beberapa Kesan Jari Yang Sama Direkonsiliasi Untuk Menghasilkan Kumpulan Minutia Yang Lebih Besar.

Proses ini, yang dikenal sebagai peningkatan templat, juga dapat digunakan untuk menghilangkan titik minutiae palsu yang mungkin ada dalam satu set fitur. Sementara pembaruan templat digunakan untuk mengakomodasi perubahan temporal dalam biometrik seseorang, tujuan peningkatan templat adalah untuk meningkatkan jumlah fitur dan mengurangi jumlah fitur palsu) sambil mempertahankan integritasnya.

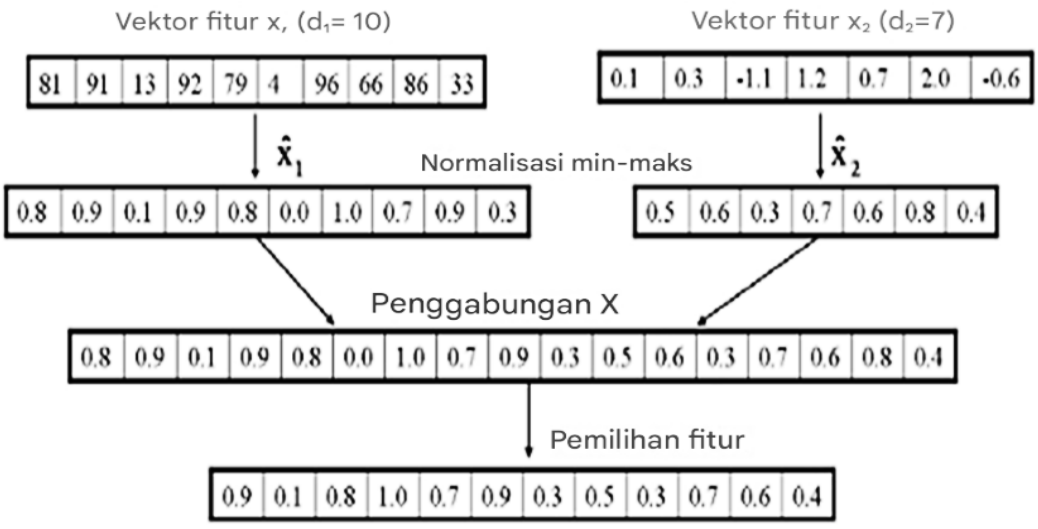
Penggabungan fitur heterogen

Bagaimana cara menggabungkan set fitur yang berasal dari berbagai algoritme dan modalitas biometrik yang berbeda? Penggabungan tingkat fitur sulit dicapai dalam kasus seperti itu karena alasan berikut:

1. Hubungan antara ruang fitur dari berbagai sistem biometrik mungkin tidak diketahui.
2. Set fitur dari berbagai modalitas mungkin tidak kompatibel. Misalnya, set minutiae sidik jari dan koefisien eigen wajah memiliki skema representasi yang berbeda. Salah satunya adalah set fitur dengan panjang variabel (yaitu, bervariasi di seluruh gambar sidik jari) yang nilai individualnya meparameterkan titik minutiae; yang lainnya adalah set fitur dengan panjang tetap (yaitu, gambar wajah direpresentasikan oleh sejumlah koefisien eigen tetap) yang nilai individualnya adalah entitas skalar.
3. Jika dua set fitur adalah vektor fitur dengan panjang tetap, maka seseorang dapat mempertimbangkan untuk menambahnya guna menghasilkan set fitur baru yang lebih besar. Namun, menggabungkan dua vektor fitur dapat menyebabkan masalah kutukan dimensionalitas, di mana peningkatan jumlah fitur sebenarnya dapat menurunkan kinerja sistem, terutama jika terdapat sedikit sampel pelatihan. Meskipun kutukan dimensionalitas merupakan masalah yang terkenal dalam pengenalan pola, hal ini khususnya terlihat jelas dalam aplikasi biometrik karena waktu, upaya, dan biaya yang diperlukan untuk mengumpulkan sejumlah besar data biometrik (pelatihan).
4. Sebagian besar sistem biometrik komersial tidak menyediakan akses ke set fitur yang digunakan dalam produk mereka karena alasan hak milik. Oleh karena itu, sangat sedikit peneliti biometrik yang berfokus pada fusi fitur heterogen dan sebagian besar dari mereka umumnya lebih menyukai skema fusi yang menggunakan skor kecocokan atau label keputusan.

Jika panjang masing-masing dari dua vektor fitur yang akan dikonsolidasikan ditetapkan di semua pengguna, maka skema penggabungan fitur diikuti oleh prosedur pengurangan dimensionalitas dapat diadopsi untuk fusi tingkat fitur. Pertimbangkan sistem multibiometrik di mana vektor fitur panjang tetap dari dua sumber biometrik tersedia, yaitu, $\mathbf{X} = \{\mathbf{x}_1, \mathbf{x}_2\}$, di mana $\mathbf{x}_1 \in \mathbb{R}^{\boldsymbol{d_1}}$ dan $\mathbf{x}_2 \in \mathbb{R}^{\boldsymbol{d_2}}$. Tujuannya adalah untuk menggabungkan kedua set fitur ini untuk menghasilkan vektor fitur baru, $\mathbf{x}_f$, yang akan lebih baik mewakili sampel biometrik seorang individu. Vektor $\mathbf{x}_f$ dari dimensionalitas $d, d < (d_1 + d_2)$ dapat dihasilkan dengan terlebih dahulu menggabungkan vektor $\mathbf{x}_1$ dan $\mathbf{x}_2$, dan kemudian melakukan pemilihan fitur atau transformasi fitur pada vektor fitur yang dihasilkan untuk mengurangi dimensionalitasnya (lihat Gambar 6.19). Tahapan utama dari pendekatan semacam itu dijelaskan di bawah ini.

Normalisasi Fitur: Nilai fitur individual dari vektor $\mathbf{x}_1 = \left[x_1^1, x_1^2, \ldots, x_1^{d_1}\right]$ dan $\mathbf{x_2} = \left[x_2^1, x_2^2, \ldots, x_2^{d_2}\right]$ dapat menunjukkan perbedaan signifikan dalam rentang dan bentuknya (yaitu, distribusi). Menambah nilai fitur yang beragam tersebut tidak akan tepat dalam banyak kasus. Misalnya, jika $\boldsymbol{x_1^i}$ berada dalam rentang [0, 100] sementara $\boldsymbol{x_2^i}$ berada dalam rentang [0, 1], maka jarak antara dua vektor fitur yang ditambah akan lebih sensitif terhadap $\boldsymbol{x_1^i}$ daripada $\boldsymbol{x_2^i}$.



Gambar 6.19 Skema Sederhana Untuk Penggabungan Dua Vektor Fitur Heterogen Yang Panjangnya Ditetapkan Untuk Semua Pengguna.

Dalam contoh ini, normalisasi min-maks dilakukan berdasarkan asumsi bahwa rentang nilai fitur adalah [0, 100] dan [-3, 3] untuk vektor fitur pertama dan kedua, berturut-turut. Tujuan normalisasi fitur adalah untuk mengubah lokasi (rata-rata) dan skala (varians) nilai fitur melalui fungsi transformasi untuk memetakannya ke domain umum. Mengadopsi skema normalisasi yang tepat juga membantu mengatasi masalah outlier dalam nilai fitur.

Normalisasi fitur mungkin tidak diperlukan dalam kasus di mana nilai fitur yang berkaitan dengan beberapa sumber sudah sebanding. Skema normalisasi sederhana yang sering digunakan dalam praktik adalah skema normalisasi min-maks, yang mengubah nilai fitur sedemikian rupa sehingga berada dalam rentang [0, 1], terlepas dari nilai aslinya. Biarkan x dan $\hat{x}$ masing-masing menunjukkan nilai fitur sebelum dan setelah normalisasi. Teknik min-max menghitung $\hat{x}$ sebagai

$$\hat{x} = \frac{x - min(h_x)}{max(h_x) - min(h_x)} \tag{6.4}$$

di mana h_x adalah fungsi yang menghasilkan x, dan min(h_x) dan max(h_x) masing-masing mewakili nilai minimum dan maksimum dari semua nilai x yang mungkin akan diamati.

Teknik min-max efektif ketika nilai minimum dan maksimum dari nilai fitur komponen diketahui sebelumnya. Dalam kasus di mana informasi tersebut tidak tersedia, estimasi parameter ini harus diperoleh dari kumpulan data pelatihan yang tersedia. Menormalkan nilai fitur menggunakan teknik normalisasi min-max menghasilkan vektor fitur yang dimodifikasi $\hat{x}_1 = \left[\hat{x}_1^1, \hat{x}_1^2, .., \hat{x}_1^{d1}\right]$ dan $\hat{x}_2 = \left[\hat{x}_2^1, \hat{x}_2^2, .., \hat{x}_2^{d2}\right]$

Salah satu keterbatasan teknik normalisasi min-max adalah sensitivitasnya terhadap outlier dalam data pelatihan. Kehadiran satu outlier, yaitu fitur yang memiliki nilai sangat tinggi atau sangat rendah dapat menyebabkan estimasi parameter maksimum atau minimum yang salah. Sejumlah teknik normalisasi telah diusulkan untuk menangani outlier secara efektif. ***Pemilihan atau Transformasi Fitur:*** Penambahan dua vektor fitur yang dinormalkan, $\hat{\mathbf{x}}_1$dan $\hat{\mathbf{x}}_2$, menghasilkan vektor fitur baru $\widehat{\mathbf{x}_f} = \hat{x}_1^1, \hat{x}_1^2, .., \hat{x}_1^{d1}, \hat{x}_2^1, \hat{x}_2^2, .., \hat{x}_2^{d2}, \hat{x}\int \in \mathbb{R}^{d1+d2}$.

Kutukan dimensionalitas mendikte bahwa vektor dimensionalitas yang diperbesar $(d_1 + d_2)$ tidak perlu menghasilkan kinerja pencocokan yang lebih baik dibandingkan dengan yang diperoleh oleh $\hat{\mathbf{x}}_1$dan $\hat{\mathbf{x}}_2$, saja. Untuk menghindari masalah ini, proses pemilihan fitur diterapkan. Pemilihan fitur adalah skema pengurangan dimensionalitas yang memerlukan pemilihan set fitur minimal berukuran $d, d < (d_1 + d_2)$, sehingga fungsi kriteria (objektif) yang diterapkan pada set pelatihan vektor fitur dioptimalkan.

Contoh algoritma pemilihan fitur meliputi pemilihan maju berurutan (SFS), pemilihan mundur berurutan (SBS), pencarian mengambang maju berurutan (SFFS), pencarian mengambang mundur berurutan (SBFS), "plus l take away r", dan pencarian cabang-dan-batas. Teknik pemilihan fitur ini bergantung pada fungsi kriteria yang diformulasikan dengan tepat untuk memperoleh subset fitur yang hampir optimal dari set fitur yang lebih besar. Dalam kasus sistem biometrik, fungsi kriteria ini bisa berupa *Equal Error Rate* (EER), total error rate, ukuran d-prime, area di bawah kurva ROC, atau GAR rata-rata pada nilai FAR yang telah ditentukan sebelumnya yang sesuai dengan set pelatihan.

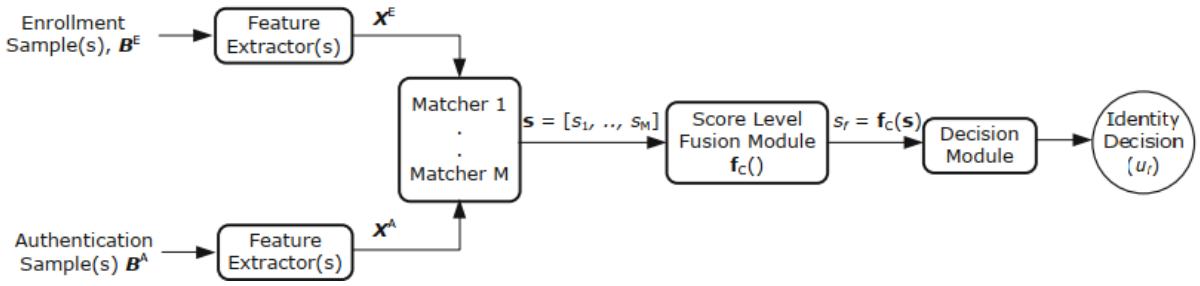
Reduksi dimensionalitas juga dapat dicapai dengan menggunakan metode transformasi fitur di mana vektor $\hat{\mathbf{x}}_f$ dikenakan pemetaan linier atau non-linier yang memproyeksikannya ke subruang berdimensi lebih rendah. Contoh transformasi tersebut meliputi penggunaan analisis komponen utama (PCA), analisis komponen independen (ICA), penskalaan multidimensi (MDS), dan Kohonen Maps. Penerapan prosedur pemilihan fitur atau transformasi fitur menghasilkan vektor fitur baru $\mathbf{x}_f = [x^1, x^2, \ldots, x^d]$, yang sekarang dapat digunakan untuk merepresentasikan sampel biometrik individu.

Penggabungan tingkat skor

Ketika skor kecocokan yang dihasilkan oleh pencocok biometrik yang berbeda digabungkan untuk mendapatkan keputusan pengenalan akhir, penggabungan dikatakan dilakukan pada tingkat skor. Ini juga dikenal sebagai penggabungan pada tingkat pengukuran atau tingkat keyakinan. Setelah data mentah dan representasi vektor fitur, tingkat penggabungan berikutnya didasarkan pada skor kecocokan. Relatif mudah untuk mengakses dan menggabungkan skor yang dihasilkan oleh pencocok biometrik yang berbeda. Akibatnya, penggabungan tingkat skor adalah pendekatan yang paling umum digunakan dalam sistem

multibiometrik. Alur informasi umum dalam sistem verifikasi multibiometrik menggunakan penggabungan tingkat skor ditunjukkan pada Gambar 6.20. Penggabungan tingkat skor merupakan masalah yang menantang ketika skor kecocokan yang dihasilkan oleh pencocok individu tidak homogen. Ketidakhomogenan dapat disebabkan oleh dua alasan berikut:

1. Satu pencocok dapat mengeluarkan ukuran jarak atau ketidaksamaan (jarak yang lebih kecil menunjukkan kecocokan yang lebih baik) sementara yang lain dapat mengeluarkan ukuran kesamaan (nilai kesamaan yang lebih besar menunjukkan kecocokan yang lebih baik). Lebih jauh, keluaran dari masing-masing pencocok tidak harus berada pada skala numerik yang sama (rentang).
2. Skor kecocokan dapat mengikuti distribusi probabilitas yang berbeda karena karakteristik masing-masing pencocok yang berbeda.

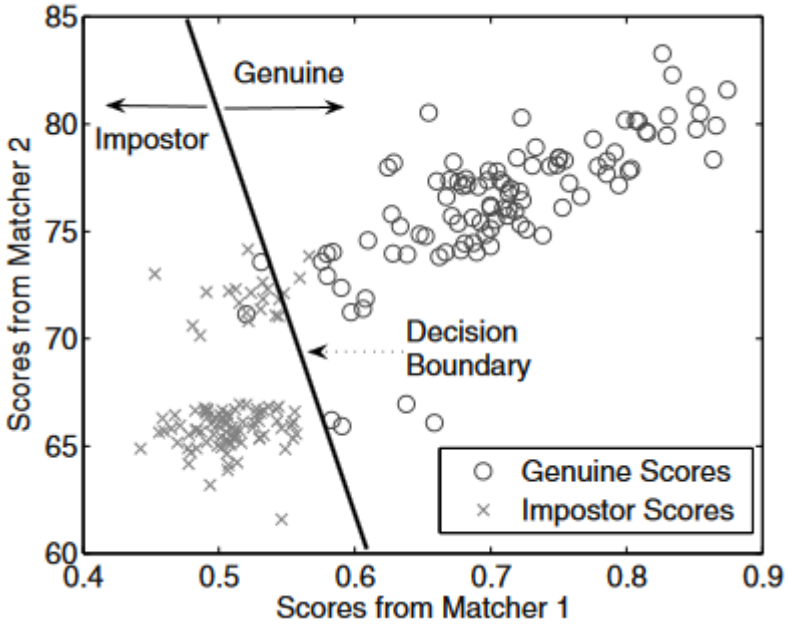


Gambar 6.20 Aliran Informasi Dalam Skema Fusi Tingkat Skor Kecocokan.

Metodologi fusi tingkat skor akan bervariasi tergantung pada apakah sistem multibiometrik beroperasi dalam mode verifikasi atau identifikasi. Fusi skor dalam sistem verifikasi multibiometrik dapat dianggap sebagai masalah klasifikasi pola dua kelas, yang tujuannya adalah untuk menentukan apakah kueri tersebut sesuai dengan pengguna asli atau penipu. Misalkan $\mathbf{s} = [s_1, s_2, \ldots, s_M]$adalah vektor skor kecocokan yang diperoleh dengan membandingkan fitur biometrik kueri $\boldsymbol{X}^A$ dengan templat terdaftar $\boldsymbol{X}^E$ menggunakan M pencocok yang berbeda. Di sini, s_M mewakili keluaran skor kecocokan oleh pencocok ke-mth.

Berdasarkan set pelatihan skor kecocokan dari kelas asli dan palsu, pengklasifikasi mempelajari batas keputusan antara kedua kelas. Gambar 6.21 menunjukkan contoh batas keputusan linier yang dipelajari oleh pengklasifikasi berdasarkan skor kecocokan asli dan palsu dari dua pencocok yang berbeda. Selama autentikasi, setiap vektor skor kecocokan yang berada di wilayah asli diklasifikasikan sebagai asli. Secara umum, batas keputusan bisa sangat rumit tergantung pada sifat pengklasifikasi.

Bergantung pada model yang digunakan untuk klasifikasi, teknik fusi skor dapat diklasifikasikan lebih lanjut ke dalam tiga kategori besar, yaitu, fusi berbasis rasio kemungkinan, fusi berbasis transformasi, dan fusi berdasarkan pendekatan klasifikasi lainnya. Namun, kategorisasi ini tidak kaku dan beberapa teknik penggabungan skor dapat dikategorikan ke dalam beberapa pendekatan atau mungkin melibatkan lebih dari satu pendekatan dasar.



Gambar 6.21 Contoh Batas Keputusan Linear Yang Dipelajari Dalam Ruang Fitur 2 Dimensi (M = 2).

Selama verifikasi, setiap vektor skor kecocokan yang berada di wilayah yang ditandai sebagai 'Asli' di sebelah kanan batas keputusan diklasifikasikan sebagai pengguna "asli". Di sisi lain, setiap vektor skor kecocokan yang berada di wilayah yang ditandai sebagai 'Penipu' di sebelah kiri batas keputusan diklasifikasikan sebagai "penipu".

Gambar 6.22 Taksonomi Pendekatan Klasifikasi Yang Dapat Digunakan Untuk Penggabungan Tingkat Skor Dalam Sistem Verifikasi Multibiometrik.

Perhatikan bahwa kategorisasi di atas tidak ketat dan beberapa teknik penggabungan skor dapat dikategorikan ke dalam beberapa pendekatan atau mungkin melibatkan lebih dari satu pendekatan dasar.

Penggabungan skor berdasarkan rasio kemungkinan

Pendekatan ini didasarkan pada teori keputusan Bayesian dan pendekatan Neyman-Pearson untuk pengujian hipotesis statistik. Demi kesederhanaan, misalkan ω_0 dan ω_1 masing-masing menunjukkan kelas penipu dan asli. Misalkan P(ω_0) dan P(ω_1) masing-masing adalah probabilitas sebelumnya untuk mengamati kelas penipu dan asli. Selanjutnya, misalkan fungsi kerapatan bersyarat untuk skor kecocokan asli dilambangkan sebagai p(s|ω_1) dan fungsi kerapatan yang sesuai untuk skor penipu dilambangkan sebagai p(s). Probabilitas posterior P(ω_j|s) dapat dihitung dari p(s|ω_j) menggunakan rumus Bayes:

$$P(\omega_j|\mathrm{s} = \frac{p(s|\omega_j)P(\omega_j)}{p(s)} \tag{6.5}$$

Dimana $j = 0{,}1\ dan\ p(s) = \sum_{j=0}^{1} p(s|\omega_j)P(\omega_j)$

Tujuannya adalah untuk memutuskan antara kelas asli dan kelas palsu berdasarkan vektor skor pertandingan yang diamati **s**. Untuk meminimalkan probabilitas kesalahan rata-rata, seseorang harus memilih kelas $\omega_j$yang memiliki probabilitas posterior tertinggi. Dengan kata lain, aturan keputusan untuk tingkat kesalahan minimum adalah:

$$Memutuskan\ \omega_1\ jika\ P(\omega_1|\mathbf{s})\ >\ \mathrm{P}(\omega_0|\mathbf{s}) \tag{6.6}$$

Aturan keputusan Bayes tingkat kesalahan minimum diperoleh dengan mensubstitusikan persamaan (6.5) ke persamaan (6.6), yang dapat dinyatakan sebagai

$$Memutuskan\ \omega_1\ jika\ P(\omega_1)\mathrm{p}(\mathrm{s}|\omega_1) >\ \mathrm{P}(\omega_0)\mathrm{p}(\mathrm{s}|\omega_0) \tag{6.7}$$

Jika probabilitas sebelumnya dari dua kelas diasumsikan sama, yaitu jika P(ω_0)= P(ω_1)= 0,5, aturan keputusan tingkat kesalahan minimum dapat disederhanakan sebagai berikut:

$$Memutuskan\ \omega_1\ jika\ \frac{p(\mathrm{p}(\mathrm{s}|\omega_1)}{p\mathrm{p}(\mathrm{s}|\omega_1)} >\ 1 \tag{6.8}$$

Statistik $p(\mathbf{s}|\omega_j)/p(\mathbf{s}|\omega_0)$dikenal sebagai rasio kemungkinan. Sementara aturan keputusan dalam persamaan (6.8) meminimalkan tingkat kesalahan total, aturan tersebut tidak banyak digunakan dalam sistem biometrik karena mengasumsikan bahwa kesalahan penerimaan salah dan penolakan salah sama-sama merugikan. Dalam sistem biometrik praktis, sering kali diinginkan untuk memiliki batas atas pada tingkat penerimaan salah. Dengan kata lain, diperlukan bahwa tingkat penerimaan salah dari sistem biometrik kurang dari, katakanlah 0,1%. Hal ini dapat dicapai dengan memodifikasi aturan keputusan dalam persamaan (6.8) berdasarkan kriteria Neyman-Pearson.

Misalkan Ψ menjadi uji statistik untuk menguji hipotesis nol H_0: s sesuai dengan penipu terhadap hipotesis alternatif H_1: s sesuai dengan pengguna asli. Misalkan Ψ (s)= j menyiratkan keputusan yang mendukung H_j, di mana j = 0, 1. Probabilitas menolak H_0 dengan benar ketika H_1 benar dikenal sebagai tingkat penerimaan asli atau daya uji. Probabilitas menolak H_0 ketika H_0 benar dikenal sebagai tingkat penerimaan salah atau tingkat uji yang dilambangkan dengan α. Teorema Neyman-Pearson menyatakan bahwa

1. Untuk menguji H_0 terhadap H1, terdapat uji Ψ dan konstanta η sehingga

$$\mathrm{P}(\Psi(\mathrm{s}) = 1|H_0 = \alpha \tag{6.9}$$

Dan

$$\Psi(\mathrm{s}) \begin{cases} 1, ketika \dfrac{p(s|\omega_1)}{p(s|\omega_1)} \geq \eta, \\ 0, ketika \dfrac{p(s|\omega_1)}{p(s|\omega_1)} < \eta \end{cases} \tag{6.10}$$

2. Jika suatu pengujian memenuhi persamaan (6.9) dan (6.10) untuk beberapa η, maka pengujian tersebut merupakan pengujian yang paling ampuh untuk menguji H_0 terhadap H_1 pada level α.

Menurut teorema Neyman-Pearson, dengan mempertimbangkan tingkat penerimaan palsu (FAR) α, pengujian optimal untuk memutuskan apakah vektor skor kecocokan s sesuai dengan pengguna asli atau penipu adalah pengujian rasio-kemungkinan. Aturan keputusan berdasarkan pengujian rasio-kemungkinan dapat dinyatakan sebagai

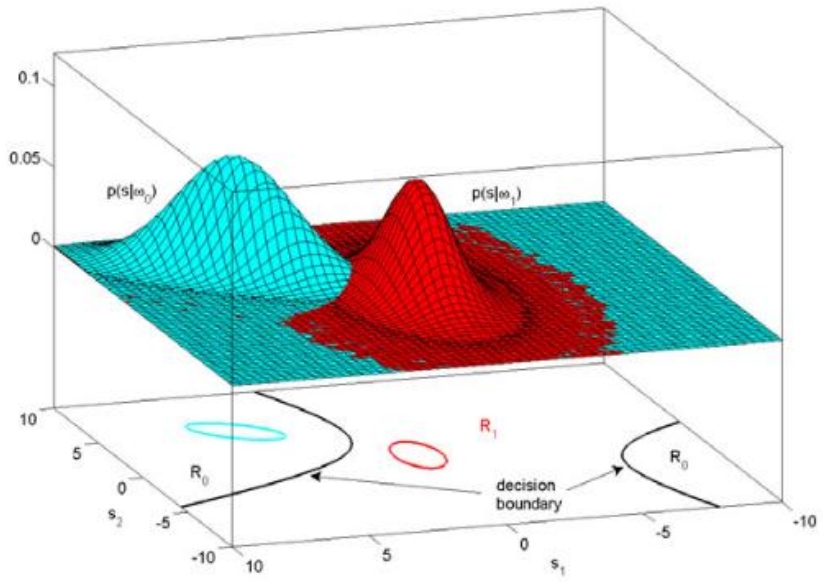
$$Memutuskan\ \omega_1\ jika\ \frac{p(s|\omega_1)}{p(s|\omega_0)} \geq \eta \tag{6.11}$$

Untuk FAR tertentu, seseorang dapat memilih ambang batas ω sedemikian rupa sehingga aturan keputusan di atas memaksimalkan tingkat penerimaan asli (GAR) dan tidak ada aturan keputusan lain dengan GAR yang lebih tinggi. Namun, keoptimalan uji rasio-kemungkinan ini dijamin hanya jika kepadatan skor kecocokan yang mendasarinya, yaitu, $p(\mathbf{s}|\omega_1)$ dan $p(\mathbf{s}|\omega_0)$ diketahui. Dalam praktiknya, hanya sekumpulan skor kecocokan asli dan palsu yang terbatas yang tersedia untuk pelatihan, sehingga kepadatan $p(\mathbf{s}|\omega_1)$ dan $p(\mathbf{s}|\omega_0)$ harus diperkirakan secara andal dari data pelatihan ini sebelum menerapkan uji rasio-kemungkinan.

Estimasi kepadatan adalah masalah yang dipelajari dengan baik dalam statistik. Dalam estimasi kepadatan parametrik, bentuk fungsi kepadatan (misalnya, Gaussian) diasumsikan diketahui dan hanya parameter fungsi kepadatan ini (misalnya, rata-rata dan deviasi standar) yang diestimasi dari data pelatihan. Misalnya, jika fungsi kepadatan diasumsikan sebagai Gaussian, hanya parameter rata-rata dan deviasi standar yang mencirikan kepadatan ini yang diestimasi selama pelatihan. Gambar 6.23 menunjukkan

batas keputusan skema fusi berbasis rasio kemungkinan dalam kasus vektor skor dua dimensi yang kepadatan kondisionalnya diasumsikan sebagai Gaussian.

Dalam konteks sistem biometrik, sangat sulit untuk memilih bentuk parametrik tertentu untuk kepadatan skor kecocokan asli dan palsu. Ini karena distribusi skor kecocokan asli dan palsu umumnya memiliki ekor yang besar dan mungkin memiliki lebih dari satu modus. Selain itu, jika bentuk parametrik untuk kerapatan skor tidak dipilih dengan hati-hati, hal itu dapat menyebabkan anomali seperti daerah keputusan yang terputus-putus. Hal ini karena rasio kemungkinan yang dihasilkan mungkin tidak monotonik sehubungan dengan skor kecocokan. Misalnya, pada Gambar 6.23, kueri akan diklasifikasikan sebagai milik kelas asli jika kedua skor kecocokan memiliki nilai positif yang besar (daerah keputusan R_0 di kiri atas R_1) serta nilai negatif yang besar (daerah keputusan R_0 di kanan bawah R_1).



Gambar 6.23 Batasan Keputusan Skema Fusi Berbasis Rasio-Kemungkinan Ketika Kerapatan Bersyarat Vektor Skor Dua Dimensi S = [S_1, S_2] Diasumsikan Sebagai Gaussian.

Di sini, $p(s|\omega_1)$ dan $p(s|\omega_0)$ masing-masing mewakili kerapatan skor kecocokan asli dan palsu. Dalam contoh ini, batas keputusan terdiri dari hiperbola, dan dengan demikian wilayah keputusan R_0 (yang sesuai dengan kelas asli) tidak terhubung. Hal ini karena rasio-kemungkinan tidak monotonik sehubungan dengan skor kecocokan. Elips menunjukkan kontur kerapatan konstan, di mana nilai kerapatan adalah 1/e kali lipat dari puncak distribusi.

Teknik estimasi kerapatan nonparametrik seperti histogram kerapatan, k-Nearest Neighbor, dan estimator kerapatan kernel (juga dikenal sebagai metode jendela Parzen) tidak mengasumsikan bentuk standar apa pun untuk fungsi kerapatan dan pada dasarnya digerakkan oleh data. Campuran kerapatan yang bentuk fungsionalnya diketahui (misalnya, campuran Gaussian) juga dapat digunakan untuk estimasi kerapatan. Metode campuran ini dapat dikategorikan sebagai parametrik atau semi-parametrik tergantung pada apakah jumlah komponen campuran ditetapkan apriori atau dibiarkan bervariasi berdasarkan data yang diamati. Meskipun pendekatan non-parametrik dan semi-parametrik dapat

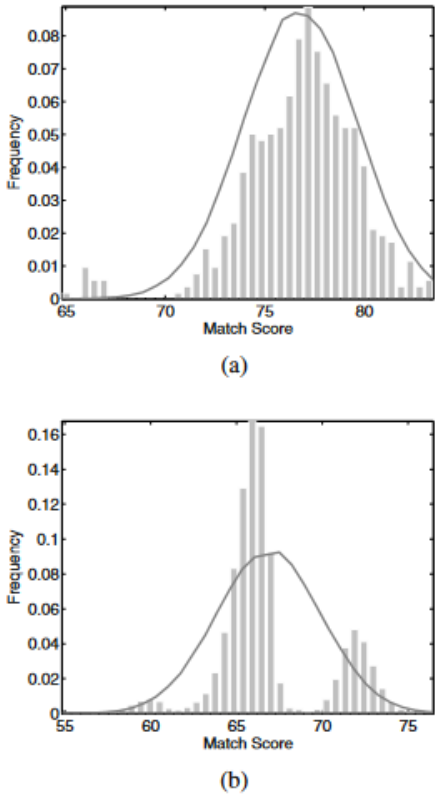
memodelkan distribusi apa pun, keandalan estimasi yang diperoleh bergantung secara signifikan pada jumlah sampel yang tersedia untuk mempelajari kepadatan, terutama jika dimensionalitas vektor skor kecocokan (M) besar.

Dalam praktiknya, hanya ada ketersediaan data pelatihan yang terbatas, terutama untuk kelas asli. Oleh karena itu, penting untuk memilih metode estimasi kepadatan yang tepat dengan hati-hati.Proses estimasi kepadatan dapat disederhanakan secara signifikan jika skor kecocokan yang dihasilkan oleh M pencocok diasumsikan secara statistik independen di bawah hipotesis H_0 dan H_1. Di bawah asumsi ini, kepadatan gabungan bersyarat $p(\mathbf{s}|\omega_j)$ dapat dinyatakan sebagai produk dari kepadatan bersyarat marginal, yaitu,

$$\mathrm{p}(\mathrm{s}|\omega_1) = \mathrm{p}(\mathrm{s1}, \mathrm{s2}, \ldots, \mathrm{sM}|\omega_j) \prod_{m-1}^{M} p(\mathrm{sM}|\omega_j), j = 0{,}1 \tag{6.12}$$

Aturan keputusan berdasarkan rasio kemungkinan dengan asumsi independensi statistik antara pencocok diberikan oleh

$$\text{Memutuskan } \omega_1 \text{ jika } \prod_{m-1}^{M}) \frac{p(\mathrm{sM}|\omega_1)}{p(\mathrm{sM}|\omega_0)} \geq \eta \tag{6.13}$$



Gambar 6.24 Histogram Skor Kecocokan Dan Estimasi Kerapatan Gaussian Yang Sesuai Untuk Pencocok Face-G Dalam Basis Data NIST BSSR1.

Gambar (a) merupakan skor asli dan gambar (b) skor penipu. Perhatikan bahwa kerapatan Gaussian tidak memperhitungkan ekor dalam distribusi skor asli dan beberapa mode dalam distribusi skor penipu. Dalam sistem biometrik multimoda, masing-masing pencocok M menggunakan fitur dari sifat biometrik yang berbeda (misalnya, wajah, sidik jari, dan geometri tangan), yang umumnya cenderung saling independen. Oleh karena itu, asumsi yang mendasari dalam Persamaan (6.12) masuk akal di sebagian besar sistem biometrik multimoda.

Di sisi lain, asumsi independensi mungkin tidak benar untuk sistem biometrik multi-sampel karena sampel yang berbeda dari sifat biometrik yang sama biasanya cenderung berkorelasi. Namun, kecuali korelasi antara pencocok sangat tinggi (katakanlah, lebih dari 0,9), degradasi akurasi sebagai akibat dari asumsi independensi tidak parah. Karena skenario ekstrem seperti itu jarang ditemui dalam sistem multibiometrik praktis, maka tepat untuk menggunakan asumsi independensi sebagai aturan praktis.

Penggabungan skor berbasis transformasi

Skema penggabungan skor berbasis transformasi biasanya merupakan perkiraan dari aturan keputusan Bayes tingkat kesalahan minimum umum yang disajikan dalam persamaan (6.7). Untuk menerapkan aturan keputusan Bayes, diperlukan estimasi probabilitas posterior $P(\omega_0|\mathbf{s})$ dan $P(\omega_1|\mathbf{s})$, yang selanjutnya memerlukan perhitungan kerapatan gabungan bersyarat $P(\mathbf{s}|\omega_0)$ dan $P(\mathbf{s}|\omega_1)$ Seperti yang disebutkan sebelumnya, memperkirakan kerapatan gabungan berdimensi-M merupakan masalah yang menantang, terutama ketika jumlah sampel pelatihan terbatas dan M besar. Perkiraan untuk $P(\omega_j|\mathbf{s})$ dapat dilakukan pada dua level.

1. Pertama, estimasi $P(\omega_j|\mathbf{s})$dapat diperoleh dengan menggunakan probabilitas posterior marginal $P, m = 1,2, \dots M$. Ini dapat dicapai dengan menggunakan berbagai aturan kombinasi pengklasifikasi yang ditunjukkan pada Tabel 6.2. Semua aturan kombinasi ini memiliki bentuk umum berikut: $P(\omega_j|\mathbf{s}) \approx \mathrm{h}(P(\omega_j|s_1), P(\omega_j|s_2), \dots, P(\omega_j|s_M))$ dan didasarkan pada dua asumsi mendasar: (a) skor kecocokan dari berbagai pencocok bersifat independen secara statistik, yaitu, persamaan (6.12) benar, dan (b) probabilitas sebelumnya dari kelas asli dan kelas penipu sama, yaitu, $P(\omega_1) = P(\omega_2) = (1/2)$ Dengan memperkirakan probabilitas posterior dalam aturan keputusan tingkat kesalahan minimum (persamaan (6.6)) menggunakan teknik kombinasi pengklasifikasi, akan diperoleh aturan keputusan berikut:

   Putuskan ω_1 jika

$$h(P(\omega_1|s_1), P(\omega_1|s_2), \dots, P(\omega_1|s_M)) > h(P(\omega_0|s_2), \dots, P(\omega_0|s_M)) \qquad (6.14)$$

   Di antara aturan kombinasi pengklasifikasi, aturan produk merupakan implikasi langsung dari asumsi bahwa skor kecocokan yang dihasilkan oleh M pencocok secara statistik independen dan kelas-kelas memiliki prior yang sama. Namun, batasan

utama dari aturan produk adalah sensitivitasnya terhadap kesalahan dalam estimasi probabilitas posterior. Bahkan jika salah satu pengklasifikasi menghasilkan probabilitas mendekati nol, produk dari M probabilitas posterior agak kecil dan ini sering kali mengarah pada keputusan klasifikasi yang salah.

Aturan jumlah umumnya lebih efektif daripada aturan produk, terutama ketika estimasi probabilitas posterior marginal tidak dapat diandalkan. Aturan jumlah dapat diturunkan dari aturan produk dengan mengasumsikan bahwa probabilitas posterior tidak menyimpang secara dramatis dari probabilitas prior untuk setiap kelas. Karena aturan keputusan jumlah kuat terhadap kesalahan dalam estimasi probabilitas posterior, aturan ini biasanya bekerja cukup baik dalam praktik dan umumnya digunakan dalam sistem multibiometrik.

Aturan maks, min, dan median juga dapat diperoleh melalui berbagai perkiraan aturan perkalian dan penjumlahan. Tabel 6.2 Aturan kombinasi pengklasifikasi mengaproksimasi probabilitas posterior gabungan $P(\omega_j|\mathrm{s} = [s_1, s_2 \dots s_M])$ menggunakan probabilitas posterior marginal $P(\omega_j|s_m), j = 0,1, m = 1,2, \dots, M$. Aturan-aturan ini memiliki bentuk umum berikut: $P(\omega_j|\mathbf{s}) \approx \mathrm{h}(P(\omega_j|s_1), P(\omega_j|s_2), \dots, P(\omega_j|s_M))$Semua aturan kombinasi ini didasarkan pada dua asumsi: (a) skor kecocokan dari pencocok yang berbeda secara statistik independen, dan (b) probabilitas sebelumnya dari kelas asli dan kelas penipu sama, yaitu, $P(\omega_0) = P(\omega_{02}) = (1/2)$.

Aturan Kombinasi	$h(P(\omega_j\|s_1), P(\omega_j\|s_2), \dots, P(\omega_j\|s_M))$
Produk	$\prod_{m=1}^{M} P(\omega_j\|s_M)$
Jumlah	$\sum_{m=1}^{M} P(\omega_j\|s_M)$
Maksimum	$max_{m=1}^{M} P(\omega_j\|s_M)$
Minimum	$min_{m=1}^{M} P(\omega_j\|s_M)$
Median	$median_{m=1}^{M} P(\omega_j\|s_M)$

2. Aturan kombinasi pengklasifikasi dapat diterapkan hanya jika keluaran setiap pencocok biometrik berbentuk $P(\omega_j|s_m)$, yaitu, probabilitas posterior kelas ω_j berdasarkan keluaran skor kecocokan oleh pencocok ke-m. Mengubah skor kecocokan menjadi probabilitas posterior marginal lagi-lagi memerlukan estimasi kepadatan skor kecocokan marginal asli dan palsu.

   Daripada menghitung kepadatan skor marginal untuk setiap pencocok, seseorang dapat mengubah skor kecocokan yang diperoleh dari pencocok yang berbeda menjadi domain umum dan langsung menerapkan aturan kombinasi pengklasifikasi pada skor yang diubah. Pendekatan ini didasarkan pada asumsi bahwa skor kecocokan dan probabilitas posterior untuk kelas asli terkait sebagai berikut.

$$P(\omega_1|s_M) \propto \mathrm{g}_m(s_m) \tag{6.15}$$

Dimana g_m adalah fungsi monotonik dan m = 1, 2, , M. Transformasi gm ini biasanya disebut sebagai fungsi normalisasi skor dan gm(sm) disebut skor kecocokan yang dinormalkan. Setelah skor kecocokan dari pencocok yang berbeda dinormalkan, aturan kombinasi pengklasifikasi seperti aturan jumlah, maks, dan min dapat diterapkan untuk mendapatkan skor kecocokan yang digabungkan. Aturan kombinasi yang sesuai disebut sebagai aturan penggabungan jumlah skor, skor maks, dan skor min, masing-masing, karena skor kecocokan yang dinormalkan mungkin tidak memiliki interpretasi probabilistik langsung (skor yang dinormalkan bahkan mungkin tidak berada dalam interval [0, 1]). Karena alasan yang sama, aturan produk umumnya tidak berlaku untuk skor yang dinormalkan. Secara umum, aturan penggabungan skor berbasis transformasi dapat dinyatakan sebagai

$$\text{Memutuskan } \omega_1 \text{ jika } \mathrm{h}(\mathrm{g}_1(\mathrm{s}_1), \mathrm{g}_2(\mathrm{s}_2), .. \mathrm{g}_\mathrm{m}(\mathrm{s}_\mathrm{m})) > \tau \tag{6.16}$$

Dimana τ adalah ambang batas keputusan yang ditetapkan oleh administrator sistem. Secara formal, normalisasi skor didefinisikan sebagai proses mengubah lokasi dan parameter skala distribusi skor pertandingan, sehingga skor pertandingan dari berbagai pencocok diubah menjadi domain umum. Lokasi dan parameter skala distribusi skor pertandingan biasanya diperkirakan dari data pelatihan. Sementara efek dari parameter lokasi adalah menerjemahkan distribusi skor sepanjang arah horizontal, efek dari parameter skala adalah meregangkan distribusi.

Jika fungsi transformasi mengubah lokasi dan parameter skala tanpa mengubah bentuk dasar distribusi, transformasi tersebut dikatakan mempertahankan distribusi skor. Beberapa skema normalisasi skor yang terkenal dirangkum dalam Tabel 6.3. Tidak ada skema normalisasi yang terbukti optimal untuk semua jenis data skor pertandingan. Dalam praktiknya, direkomendasikan agar sejumlah teknik normalisasi dievaluasi untuk menentukan salah satu yang memberikan kinerja terbaik pada data yang diberikan. Fungsi ψ dalam normalisasi tanh dikenal sebagai fungsi pengaruh Hampel, dan fungsi ini mengurangi pengaruh skor pada ekor distribusi selama estimasi parameter lokasi dan skala. Dalam tabel ini, diasumsikan bahwa parameter lokasi dan skala suatu distribusi dapat diestimasi dari serangkaian skor pelatihan $\{\hat{s}_m^i\}$ yang diberikan, untuk $m = 1, 2, \cdots, M$ dan $i = 1, 2, \cdots, L1$, (L_1 + 1), (L_1 + 2), , (L_1 + L_0). Di sini, $\hat{s}_m^i$merepresentasikan skor ke-ith dalam set pelatihan yang sesuai dengan pencocok ke-m. Diasumsikan juga bahwa skor L_1 pertama dalam set pelatihan sesuai dengan kelas asli, skor L_0 berikutnya sesuai dengan kelas penipu, dan jumlah total sampel pelatihan adalah L, yaitu, L = L_1 + L_0.

Skema normalisasi	**Fungsi normalisasi $G(s_m)$**	**Parameter lokasi (μm)**	**Parameter skala ($\sigma\eta$)**
Min-Maks	$\frac{s_m - \mu_m}{\sigma_m}$	$min_{i=1}^{L}\, \hat{s}_m^i$	$\left(max_{i=1}^{L}\, \hat{s}_m^i\right) - \mu m$

Skor Z	$\frac{s_m - \mu_m}{\sigma_m}$	$\frac{1}{L}\sum_{i=1}^{L} \hat{s}_m^i$	$\frac{1}{L}\sum_{i=1}^{L} (\hat{s}_m^i - \mu m)$
Median	$\frac{s_m - \mu_m}{\sigma_m}$	$median_{i=1}^{L}\, \hat{s}_m^i$	$median_{i=1}^{L}\, \lvert\hat{s}_m^i - \mu m\rvert$
Tanh	$\frac{1}{2}\left\{\tan\left(0.01\left(\frac{s_m - \mu_m}{\sigma_m}\right)\right) + 1\right\}$	$\frac{1}{L_1}\sum_{i=1}^{L_1} \Psi\, \hat{s}_m^i$	$\frac{1}{L_1}\sum_{i=1}^{L_1} (\Psi\, (\hat{s}_m^i - \mu m)^2$

Teknik normalisasi yang paling sederhana adalah normalisasi min-maks. Normalisasi min-maks paling cocok untuk kasus di mana batas (nilai maksimum dan minimum) skor yang dihasilkan oleh pencocok diketahui. Dalam kasus ini, seseorang dapat dengan mudah mengubah skor minimum dan maksimum menjadi 0 dan 1, berturut-turut. Namun, bahkan jika skor kecocokan tidak dibatasi, normalisasi min-maks dapat diterapkan berdasarkan nilai minimum dan maksimum yang diestimasikan dari kumpulan skor kecocokan pelatihan yang diberikan. Namun metode ini sangat sensitif terhadap outlier dalam data pelatihan. Normalisasi min-maks mempertahankan bentuk asli dari distribusi skor kecuali untuk faktor skala dan mengubah semua skor menjadi rentang umum [0, 1]. Skor jarak dapat diubah menjadi skor kesamaan dengan mengurangi skor yang dinormalisasi dari 1. Teknik normalisasi skor lain yang umum digunakan adalah normalisasi skor-z yang menggunakan rata-rata aritmatika dan deviasi standar dari data pelatihan. Sekali lagi, statistik rata-rata dan deviasi standar sensitif terhadap outlier dalam data pelatihan. Normalisasi skor-Z tidak menjamin rentang numerik umum untuk skor yang dinormalkan dari berbagai pencocok. Statistik median dan deviasi absolut median (MAD) tidak peka terhadap outlier serta titik-titik di ekor ekstrem distribusi. Namun, ketika distribusi skor bukan Gaussian, median dan MAD merupakan estimasi yang buruk dari parameter lokasi dan skala. Oleh karena itu, teknik normalisasi ini tidak mengubah skor menjadi rentang numerik umum. Normalisasi tanh menggunakan estimasi mean dan deviasi standar hanya dari skor asli sebagaimana diberikan oleh estimator Hampel. Estimator Hampel didasarkan pada fungsi pengaruh (ψ) berikut:

$$\psi(u) = \begin{cases} u & 0 \le |u| < a, \\ a * sign(u) & a \le |u| < b, \\ a * sign(u) * \left(\frac{c - |u|}{c - b}\right) & b \le |u| < c, \\ 0 & |u| \ge c, \end{cases} \tag{6.17}$$

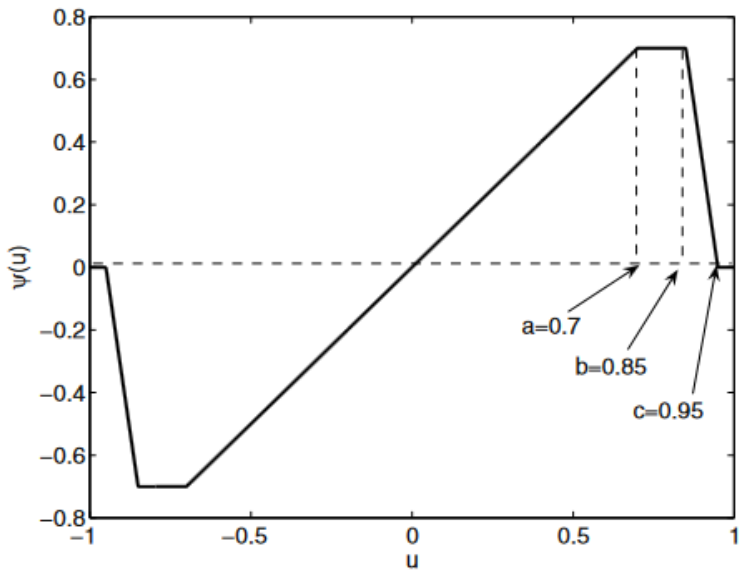
Dimana

$$sign\{u\} = \begin{cases} +1, \text{ if } u \ge 0, \\ -1, \text{ otherwise.} \end{cases}$$

Plot fungsi pengaruh Hampel ditunjukkan pada Gambar 6.25. Fungsi pengaruh Hampel mengurangi pengaruh skor pada ekor distribusi (diidentifikasi oleh a, b, dan c) selama estimasi parameter lokasi dan skala. Oleh karena itu, metode ini tidak sensitif

terhadap outlier. Namun, jika banyak titik yang membentuk ekor distribusi dibuang, estimasi mungkin tidak akurat. Oleh karena itu, parameter a, b, dan c harus dipilih dengan hati-hati tergantung pada jumlah gangguan dalam data pelatihan yang tersedia. Di antara berbagai teknik fusi skor berbasis transformasi yang tersedia, aturan keputusan jumlah skor adalah teknik yang paling umum digunakan dalam sistem multibiometrik. Aturan keputusan ini sering digunakan bersama dengan teknik normalisasi min-max atau z-score. Meskipun aturan jumlah skor sederhana, aturan ini juga cukup kuat terhadap variasi skor pencocok individu, dan inilah alasan penggunaannya yang luas.

Modifikasi aturan jumlah skor adalah aturan jumlah skor terbobot (atau sederhananya, aturan jumlah terbobot), di mana skor pencocokan gabungan dihitung sebagai jumlah terbobot dari skor yang dinormalkan dari pencocokan individu. Alasan di balik aturan jumlah terbobot adalah karena perbedaan dalam distribusi skor dari pencocokan individu, konstanta proporsionalitas dalam persamaan (6.15) mungkin tidak sama untuk semua m = 1, 2, , M. Bobot diberikan pada skor pencocokan individu untuk mengatasi masalah ini dan bobot ini sering dipilih untuk mengoptimalkan beberapa kriteria seperti tingkat kesalahan yang sama atau area di bawah kurva ROC.



Gambar 6.25 Contoh Fungsi Pengaruh Hampel Dengan A = 0,7, B = 0,85, Dan C = 0,95.

Penggabungan skor berdasarkan pendekatan klasifikasi lain

Sejumlah pendekatan klasifikasi lain dapat digunakan untuk secara tidak langsung mempelajari batas keputusan antara skor asli dan palsu. Beberapa contohnya meliputi *support vector machines* (SVM), jaringan saraf, k-nearest neighbor classifier, analisis diskriminan linier, pohon keputusan, dan random forest. Analisis terperinci dari berbagai model diskriminatif berada di luar cakupan buku ini. Namun, dalam konteks sistem biometrik, penting untuk mempertimbangkan dua masalah berikut saat memilih model diskriminatif yang tepat:

a. Set pelatihan tidak seimbang: Jumlah skor kecocokan asli yang tersedia untuk pelatihan adalah O(N), tetapi jumlah skor penipu adalah O(N^2), di mana N adalah jumlah pengguna dalam basis data pelatihan. Misalnya, jika basis data pelatihan multibiometrik memiliki N pengguna dan jika setiap pengguna menyediakan t sampel biometrik, maka jumlah maksimum skor asli yang dapat diperoleh dari basis data ini adalah $Nt(t-1)/2$. Di sisi lain, kecocokan penipu $(N(N-1)t^2)/2$ dapat dilakukan menggunakan basis data yang sama. Misalkan N = 100 dan t = 4, jumlah skor asli yang tersedia untuk pelatihan hanya 600, sedangkan jumlah skor penipu adalah 79.200.
b. Biaya kesalahan klasifikasi: Bergantung pada aplikasi biometrik, biaya menerima penipu mungkin sangat berbeda dari biaya menolak pengguna asli. Misalnya, sistem biometrik yang diterapkan dalam aplikasi keamanan mungkin diharuskan memiliki rasio penerimaan palsu (FAR) kurang dari 0,1%. Oleh karena itu, strategi fusi perlu meminimalkan rasio penolakan palsu (FRR) pada nilai FAR yang ditentukan daripada meminimalkan rasio kesalahan total (jumlah FAR dan FRR).

Penggabungan skor dalam mode identifikasi

Perbedaan utama antara penggabungan skor dalam mode verifikasi dan identifikasi adalah struktur data skor kecocokan dan keputusan keluaran. Dalam sistem verifikasi, data skor berbentuk vektor $s = [s_1, s_2, \dots, s_M]$, di mana sm mewakili keluaran skor kecocokan oleh pencocok ke-m dan sesuai dengan satu identitas yang diklaim. Tujuannya adalah untuk menentukan apakah klaim identitas berasal dari pengguna "asli" atau "penipu" berdasarkan s. Di sisi lain, data skor dalam sistem identifikasi berbentuk matriks $N \times M\ S = [s_{n,m}]$di mana $s_{n,m}$ adalah keluaran skor kecocokan oleh pencocok ke-m yang sesuai dengan identitas ke-n.

Dalam kasus ini, tujuannya adalah untuk menetapkan identitas I_k kepada pengguna berdasarkan matriks skor S. Dengan sedikit modifikasi, banyak aturan keputusan yang dirancang untuk skenario verifikasi juga dapat diperluas ke mode identifikasi. Namun, tidak mudah untuk menerapkan skema fusi berdasarkan model diskriminatif lain ke skenario identifikasi. Ini karena identifikasi multibiometrik adalah masalah klasifikasi pola multikelas, di mana jumlah kelas (N) bisa sangat besar. Pertama, aturan keputusan tingkat kesalahan minimum untuk mode identifikasi adalah:

$$Menentukan\ identitas\ l_k\ jika\ P(l_k|\mathrm{S}) > \mathrm{P}(\ l_n|\mathrm{S}), \forall\ \mathrm{n} = 1,2,\dots,\mathrm{N}, \mathrm{k}\ \neq \mathrm{n}, \qquad (6.18)$$

Dimana $\mathrm{P}(\ l_n|\mathrm{S})$, adalah probabilitas posterior bahwa identitas pengguna adalah l_n yang diberikan matriks skor S. Dengan menerapkan rumus Bayes, aturan keputusan Bayes dengan tingkat kesalahan minimum dapat diperoleh sebagai

$$Menentukan\ identitas\ l_k\ jika\ P(l_k)\mathrm{p}(\mathrm{S}|l_k) > \mathrm{P}(\ l_n)\mathrm{p}(\mathrm{S}|l_n), \forall\ \mathrm{n} = 1,2,\dots,\mathrm{N}, \mathrm{k}\ \neq \mathrm{n}, \quad (6.19)$$

Di mana $\mathrm{P}(S|l_n)$ adalah kemungkinan mengamati matriks skor S jika identitas sebenarnya adalah l_n dan $P(l_n)$ adalah probabilitas sebelumnya untuk mengamati identitas In. Jika probabilitas sebelumnya untuk semua pengguna diasumsikan sama, yaitu, jika

$P(l_n) = \left(\frac{1}{N}\right), \forall n = 1,2,\ldots,N$, aturan keputusan tingkat kesalahan minimum dapat disederhanakan sebagai berikut:

$$Menentukan\ identitas\ l_k\ jika\ p(l_k) > \mathrm{p(S|}l_n), \forall\ \mathrm{n} = 1,2,\ldots,\mathrm{N}, \mathrm{k}\ \neq \mathrm{n}, \qquad (6.20)$$

Idealnya, kerapatan bersyarat **S** harus diestimasi secara individual untuk setiap pengguna karena ia menangkap informasi lengkap tentang ketergantungan antara skor yang diberikan kepada pengguna yang berbeda dan karakteristik khusus pengguna dari skor kecocokan. Namun, memperkirakan kerapatan bersyarat S secara langsung tidaklah praktis karena dua alasan berikut:

a. Karena **S** adalah matriks berdimensi N M dan N biasanya cukup besar dalam skenario identifikasi (dalam orde puluhan juta), memperkirakan kerapatan **S** memerlukan sejumlah besar sampel pelatihan untuk setiap pengguna, yang tidak layak
b. Kerapatan **S** perlu diestimasi ulang secara berkala karena perubahan dalam daftar pendaftar.

Jika skor kecocokan untuk orang yang berbeda diasumsikan independen secara statistik, kemungkinan $\mathrm{p(S|l_n)}$ dapat disederhanakan sebagai

$$\mathrm{p(S|l_n)} = \prod_{\mathrm{j-1}}^{\mathrm{N}} \mathrm{p(s_j,|l_n)} = \mathrm{p(s_n|l_n)} \prod_{\mathrm{j=1,j\neq n}}^{\mathrm{N}} \mathrm{p(s_j,l_n)} \qquad (6.21)$$

Di sini, sn,. mewakili baris ke-n dari matriks skor $\mathbf{S}, \mathrm{p(s_n|l_n)}$) adalah kepadatan skor kecocokan asli yang sesuai dengan pengguna In dan $\mathrm{p(s_n|l_n)}$, $j\ \neq\ n$ adalah kepadatan skor penipu ketika identitas yang diklaim adalah l_n. Namun, ketika skor kecocokan asli (penipu) dari semua pengguna diasumsikan terdistribusi secara identik, $\mathrm{p(s_n|l_n)}$= $\mathrm{p(s,\omega}_1)$ dan $\mathrm{p(s_j|l_n)}$= p $\mathrm{p(s,|\omega}_0)$, $\mathrm{j}\ =\ 1,2,,\mathrm{N}$, dan asumsi j, persamaan (6.21) dapat disederhanakan lebih lanjut sebagai

$$\mathrm{p(S|l_n)} = \mathrm{p(s_n,\omega}_1) \prod_{\mathrm{j=1,j\neq n}}^{\mathrm{N}} \mathrm{p(s_j,\ \omega_0)} = \frac{\mathrm{p(s_n,|\omega}_1)}{\mathrm{p(s_n,|\omega}_0)} \prod_{\mathrm{j=1}}^{\mathrm{N}} \mathrm{p(s_j,|\omega}_1) \qquad (6.22)$$

Sekarang, kemungkinan mengamati matriks skor S jika identitas sebenarnya adalah In adalah proporsional dengan rasio kemungkinan yang digunakan dalam skenario verifikasi. Oleh karena itu, aturan keputusan tingkat kesalahan minimum dapat disederhanakan sebagai

$$\text{Menentukan identitas } \mathrm{I_k} \text{ jika } \frac{\mathrm{p(s_k,\omega}_1)}{\mathrm{p(s_k,\omega}_0)} > \frac{\mathrm{p(s_n,\omega}_1)}{\mathrm{p(s_n,\omega}_1)}, \forall \mathrm{n} = 1,2,\ldots,\mathrm{N} \qquad (6.23)$$

Lebih jauh lagi, jika skor dari pencocok yang berbeda diasumsikan independen secara kondisional, seseorang dapat memperkirakan kepadatan gabungan dari skor kecocokan asli

(peniru) dengan hasil perkalian kepadatan marginal. Oleh karena itu, aturan keputusan dalam persamaan (6.23) dapat dinyatakan kembali sebagai

$$\text{Menentukan identitas } I_k \text{ jika } \prod_{m-1}^{M} \frac{p(s_{k,m}, \omega_1)}{p(s_{k,m}, \omega_0)} > \prod_{m=1}^{M} \frac{p(s_n, \omega_1)}{p(s_n, \omega_0)}, \forall n = 1,2, \dots, N \qquad (6.24)$$

Persamaan (6.23) dan (6.24) dapat dianggap sebagai aturan keputusan berbasis rasio kemungkinan untuk skenario identifikasi. Demikian pula, skema fusi skor berbasis transformasi juga dapat diperluas untuk identifikasi. Misalnya, aturan keputusan jumlah skor untuk identifikasi multibiometrik dapat dinyatakan sebagai berikut:

$$\text{Menentukan identitas } I_k \text{ jika } \sum_{m=1}^{M} g_m(s_{k,m}) > \sum_{m=1}^{M} g_m(s_{n,m}), \forall n = 1,2, \dots, N \qquad (6.25)$$

Penggabungan skor berbasis kualitas

Kualitas data biometrik yang diperoleh secara langsung memengaruhi kemampuan pencocok biometrik untuk melakukan proses pencocokan secara efektif. Memperkirakan kualitas sampel biometrik dan memprediksi kinerja pencocok biometrik berdasarkan kualitas yang diestimasikan dapat sangat berguna dalam membangun sistem multibiometrik yang tangguh. Ini akan memungkinkan penugasan bobot yang dinamis kepada pencocok biometrik individual berdasarkan kualitas sampel input yang akan diverifikasi.

Misalnya, pertimbangkan sistem bimodal dengan iris dan sidik jari sebagai dua modalitas. Misalkan selama upaya akses tertentu oleh pengguna, citra iris berkualitas buruk tetapi kualitas citra sidik jari cukup baik. Dalam hal ini, bobot yang lebih tinggi dapat diberikan pada skor pencocokan sidik jari dan bobot yang lebih rendah pada skor pencocokan iris. Salah satu metode untuk melakukan penggabungan berbasis kualitas adalah dengan memasukkan kualitas sampel ke dalam kerangka penggabungan skor berbasis rasio kemungkinan.

Karena sampel berkualitas buruk akan sulit diklasifikasikan sebagai asli atau palsu (lihat Gambar 6.26), rasio kemungkinan untuk sampel tersebut akan mendekati 1. Di sisi lain, untuk sampel berkualitas baik, rasio kemungkinan akan lebih besar dari 1 untuk pengguna asli dan kurang dari 1 untuk palsu. Oleh karena itu, rasio kemungkinan yang dihasilkan dari penggunaan kepadatan gabungan skor kecocokan dan kualitas terkait akan dibobot secara implisit oleh kualitas sampel masing-masing. Jika pencocok biometrik M diasumsikan independen, aturan fusi rasio kemungkinan berbasis kualitas dapat dinyatakan sebagai berikut:

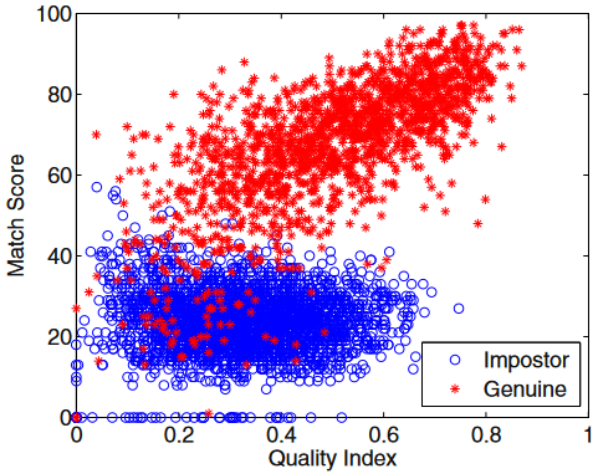
$$Menentukan\ \omega_1\ jika\ \prod_{M=1}^{M} \frac{p(s_m, q_m|\ \omega_1)}{p(s_m, q_m|\ \omega_0)} \geq \eta \qquad (6.26)$$

Di mana qm adalah kualitas kecocokan yang disediakan oleh pencocokan ke-m, untuk m = 1,..., m, p(sm, qm ω1) dan p(sm, qm ω 0) adalah kepadatan gabungan dari skor kecocokan dan kualitas yang diperkirakan dari skor pelatihan asli dan palsu, masing-masing, dari pencocokan ke-m. Informasi kualitas juga dapat dimasukkan ke dalam skema fusi berbasis transformasi dan metode berdasarkan model diskriminatif lainnya. Misalnya, data kualitas dapat digunakan untuk secara dinamis mengubah bobot yang ditetapkan ke pencocok yang berbeda dalam aturan jumlah tertimbang. Demikian pula, nilai kualitas dapat digunakan untuk mengubah biaya kesalahan klasifikasi saat melatih pengklasifikasi support vector machine (SVM).

Fusi tingkat peringkat

Ketika sistem biometrik beroperasi dalam mode identifikasi, keluaran sistem dapat dilihat sebagai peringkat identitas yang terdaftar. Dalam kasus ini, output menunjukkan himpunan kemungkinan identitas yang cocok yang diurutkan dalam urutan menurun dari tingkat keyakinan. Sasaran skema fusi tingkat peringkat adalah untuk mengkonsolidasikan semua peringkat yang dikeluarkan oleh masing-masing subsistem biometrik untuk memperoleh peringkat konsensus untuk setiap identitas.

Peringkat memberikan lebih banyak wawasan tentang proses pengambilan keputusan pencocok dibandingkan dengan hanya identitas kecocokan terbaik, tetapi peringkat mengungkapkan lebih sedikit informasi daripada skor kecocokan. Namun, tidak seperti skor kecocokan, peringkat yang dikeluarkan oleh beberapa sistem biometrik dapat dibandingkan. Akibatnya, tidak diperlukan normalisasi dan ini membuat skema fusi tingkat peringkat lebih mudah diimplementasikan dibandingkan dengan teknik fusi tingkat skor.



Gambar 6.26 Variasi Skor Kecocokan Berkenaan Dengan Kualitas Gambar Untuk Modalitas Sidik Jari (Diadaptasi Dari [22]).

Perhatikan bahwa skor kecocokan asli dan palsu dipisahkan dengan baik hanya untuk sampel berkualitas baik (dengan indeks kualitas > 0,5). Distribusi skor yang diamati mungkin berbeda jika pencocok sidik jari atau indeks kualitas yang berbeda digunakan. Misalkan **R** = [$r_{n,m}$]

adalah matriks peringkat dalam sistem multibiometrik, di mana rn,m adalah peringkat yang ditetapkan untuk identitas I_n oleh pencocok,$\mathrm{mth}, \mathrm{m} = 1, \cdots, \mathrm{M}$ dan n = 1,⋯, N.

Misalkan $\hat{r}_n$ adalah statistik yang dihitung untuk pengguna In sehingga pengguna dengan nilai $\hat{r}$ terendah ditetapkan peringkat konsensus tertinggi (atau diurutkan ulang). Tiga metode terkenal berikut dapat digunakan untuk menghitung statistik $\hat{r}$. Dalam metode peringkat tertinggi, setiap pengguna ditetapkan peringkat tertinggi (nilai r minimum) sebagaimana dihitung oleh pencocok yang berbeda, yaitu, statistik untuk pengguna In adalah

$$\hat{r}_n = \min_{m=1}^{M} r_{n,m}. \tag{6.27}$$

Hasil seri diputus secara acak untuk mendapatkan urutan peringkat yang ketat. Metode ini hanya berguna jika jumlah pengguna lebih banyak dibandingkan dengan jumlah pencocok, yang biasanya terjadi dalam sistem identifikasi biometrik. Jika kondisi ini tidak terpenuhi, sebagian besar pengguna akan memiliki hasil seri sehingga peringkat akhir tidak informatif. Keuntungan dari metode peringkat tertinggi adalah dapat memanfaatkan kekuatan setiap pencocok secara efektif.

Bahkan jika hanya satu pencocok yang memberikan peringkat tinggi kepada pengguna yang benar, masih sangat mungkin bahwa pengguna yang benar akan menerima peringkat tinggi setelah pengurutan ulang. Metode Hitung Borda: Metode hitungan Borda menggunakan jumlah peringkat yang diberikan oleh masing-masing pencocok untuk menghitung nilai $\hat{r}$, yaitu, statistik untuk pengguna In adalah

$$\hat{r}_n = \sum_{m=1}^{M} r_{n,m} \tag{6.28}$$

Besarnya hitungan Borda untuk setiap pengguna adalah ukuran derajat persetujuan di antara berbagai pencocok mengenai apakah input tersebut milik pengguna tersebut. Metode hitungan Borda mengasumsikan bahwa peringkat yang diberikan kepada pengguna oleh pencocok bersifat independen secara statistik dan semua pencocok memiliki kinerja yang sama baiknya. Metode regresi logistik adalah generalisasi dari metode hitungan Borda di mana jumlah bobot dari peringkat individual dihitung, yaitu, statistik untuk pengguna In adalah

$$\hat{r}_k = \sum_{m=1}^{M} w_m r_{n,m} \tag{6.29}$$

Bobot, w_m , yang akan ditetapkan pada pencocok ke-mth, m = 1,... , M, ditentukan oleh regresi logistik. Metode regresi logistik berguna ketika pencocok biometrik yang berbeda memiliki perbedaan signifikan dalam akurasinya. Salah satu keterbatasan metode ini adalah memerlukan fase pelatihan untuk menentukan bobot. Untuk citra wajah kueri tertentu, dua algoritme pengenalan wajah memberi peringkat empat pengguna dalam basis data berdasarkan kesamaan mereka. Kolom skor yang digabungkan pada Gambar 6.27 menunjukkan nilai r_n. Ketika metode peringkat tertinggi digunakan, ada seri untuk peringkat 1 antara pengguna "Alice" dan "Bob". Dalam contoh ini, peringkat yang diurutkan ulang diperoleh dengan memutus seri secara acak.

Face Matcher 1

User Identity	Rank
Alice	3
Bob	**1**
Charlie	4
Dick	2

Face Matcher 2

User Identity	Rank
Alice	**1**
Bob	2
Charlie	3
Dick	4

Rank Fusion Module

	Highest Rank		Borda Count		Logistic Regression (w_1 = 0.8, w_2 = 0.2)	
User Identity	Fused Score	Reordered Rank	Fused Score	Reordered Rank	Fused Score	Reordered Rank
Alice	**1**	**1**	4	2	2.6	3
Bob	1	2	**3**	**1**	**1.2**	**1**
Charlie	3	4	7	4	3.8	4
Dick	2	3	6	3	2.4	2

Gambar 6.27 Ilustrasi Penggabungan Tingkat Peringkat Yang Dilakukan Dengan Metode Peringkat Tertinggi, Hitungan Borda, Dan Regresi Logistik

Karena peringkat tertinggi dan metode hitungan Borda mengasumsikan bahwa kedua pencocok wajah bekerja dengan baik, peringkat yang disusun ulang cenderung merupakan campuran peringkat yang ditetapkan secara individual oleh kedua pencocok. Di sisi lain, metode regresi logistik menetapkan bobot yang lebih tinggi pada peringkat yang diberikan oleh pencocok yang lebih akurat. Akibatnya, peringkat yang disusun ulang dapat diharapkan serupa dengan peringkat yang diberikan oleh pencocok dengan akurasi yang lebih tinggi.

Dalam contoh yang ditunjukkan pada Gambar 6.27, pencocok 1 lebih akurat daripada pencocok 2. Oleh karena itu, bobot 0,8 diberikan padanya dan karena perbedaan bobot yang signifikan ini, peringkat yang disusun ulang dalam kasus regresi logistik sama persis dengan peringkat yang diberikan oleh pencocok 1.

Dalam contoh ini, ketiga skema penggabungan menetapkan peringkat konsensus yang berbeda untuk identitas individual.

Penggabungan tingkat keputusan

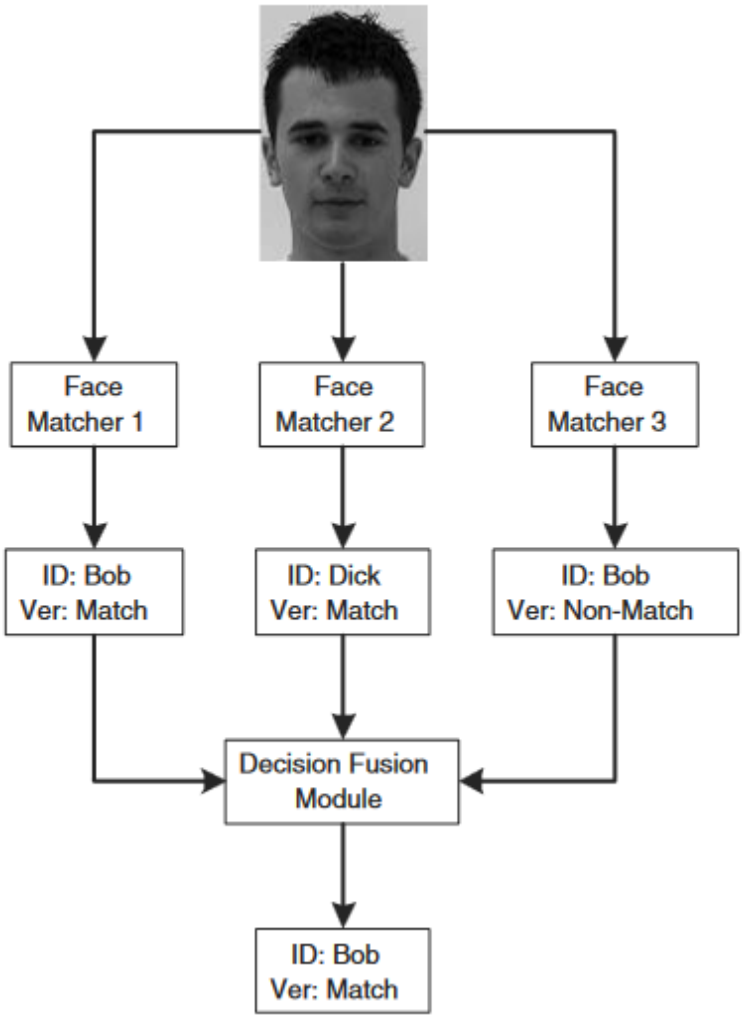
Dalam sistem multibiometrik, penggabungan dilakukan pada tingkat abstrak atau tingkat keputusan ketika hanya keputusan yang dihasilkan oleh pencocok biometrik individual yang tersedia. Misalnya, banyak pencocok biometrik komersial siap pakai (COTS) yang hanya menyediakan akses ke keputusan pengenalan akhir. Ketika pencocok COTS tersebut digunakan untuk membangun sistem multibiometrik, hanya penggabungan tingkat keputusan yang layak. Metode yang diusulkan dalam literatur untuk penggabungan tingkat keputusan meliputi aturan “AND” dan “OR”, pemungutan suara mayoritas, pemungutan suara mayoritas tertimbang, penggabungan keputusan Bayesian, teori bukti Dempster-Shafer, dan ruang pengetahuan perilaku.

Aturan “AND” dan “OR”: Dalam sistem verifikasi multibiometrik, metode paling sederhana untuk menggabungkan keputusan yang dihasilkan oleh pencocok yang berbeda adalah dengan menggunakan aturan AND dan OR. Keluaran aturan AND adalah “kecocokan” hanya ketika semua pencocok biometrik M setuju bahwa sampel masukan cocok dengan templat. Sebaliknya, aturan OR menghasilkan keputusan "cocok" selama setidaknya satu dari M pencocok memutuskan bahwa sampel input cocok dengan templat. Keterbatasan kedua aturan ini adalah kecenderungannya untuk menghasilkan titik operasi yang ekstrem. Ketika aturan AND diterapkan, False Accept Rate (FAR) dari sistem multibiometrik sangat rendah (lebih rendah daripada FAR dari pencocok individu) sementara False Reject Rate (FRR) tinggi (lebih besar daripada FRR dari pencocok individu).

Demikian pula, aturan OR menghasilkan FAR yang lebih tinggi dan FRR yang lebih rendah daripada pencocok individu. Ketika satu pencocok biometrik memiliki tingkat kesalahan yang sama yang jauh lebih tinggi dibandingkan dengan pencocok lainnya, kombinasi dari dua pencocok yang menggunakan aturan AND dan OR sebenarnya dapat menurunkan kinerja keseluruhan. Karena fenomena ini, aturan fusi keputusan AND dan OR jarang digunakan dalam sistem multibiometrik praktis. Pemungutan Suara Mayoritas: Pendekatan yang paling umum untuk penggabungan tingkat keputusan adalah pemungutan suara mayoritas di mana sampel biometrik input ditetapkan ke kelas tersebut (“asli” atau “peniru” untuk sistem verifikasi dan identitas Ik untuk sistem identifikasi) yang disetujui oleh mayoritas pencocok. Jika ada M pencocok biometrik, sampel input ditetapkan ke kelas jika setidaknya $\hat{m}$ pencocok setuju pada kelas tersebut, di mana

$$\hat{m}\begin{cases}\frac{M}{2}+1\ jika\ M\\ \frac{m+1}{2}\ ketika\end{cases} \tag{6.30}$$

Ketika tidak ada kelas yang didukung oleh mˆ matcher, keputusan “tolak” dikeluarkan oleh sistem. Pemungutan suara mayoritas mengasumsikan bahwa semua matcher bekerja dengan baik. Keuntungan dari pemungutan suara mayoritas adalah: (a) tidak diperlukan pengetahuan apriori tentang matcher, dan (b) tidak diperlukan pelatihan untuk menghasilkan keputusan akhir. Contoh yang ditunjukkan pada Gambar 6.28 adalah ilustrasi sederhana dari skema pemungutan suara mayoritas, di mana tiga matcher pengenalan wajah digunakan. Dalam mode identifikasi, dua dari tiga matcher mengidentifikasi pengguna sebagai “Bob”. Oleh karena itu, keputusan identitas akhir setelah penggabungan juga adalah “Bob”. Demikian pula, dalam mode verifikasi, karena dua dari tiga matcher memutuskan bahwa gambar wajah input cocok dengan templat identitas yang diklaim, yaitu “Bob”, keputusan akhir setelah penggabungan adalah “asli”.



Gambar 6.28 Aliran Informasi Saat Keputusan Yang Diberikan Oleh Beberapa Pencocok Biometrik Digabungkan Menggunakan Skema Fusi Suara Mayoritas

Di sini, "ID" dan "Ver" masing-masing mewakili mode identifikasi dan verifikasi operasi pengenalan. Untuk mode verifikasi, identitas yang diklaim adalah Bob. Pemungutan Suara Mayoritas Tertimbang: Saat pencocok yang digunakan dalam sistem multibiometrik tidak memiliki akurasi pengenalan yang sama, masuk akal untuk menetapkan bobot yang lebih tinggi pada keputusan yang dibuat oleh pencocok yang lebih akurat. Untuk memfasilitasi pembobotan ini, label yang dikeluarkan oleh masing-masing pencocok

$$\tilde{s}_{n,m} = \begin{cases} 1, jika\ output\ pada\ m^{th} matcher\ adalah\ kelas\ n \\ 0, \end{cases} \quad (6.31)$$

dimana m = 1,..., M dan n = 0, 1 untuk verifikasi atau n = 1, 2, , N untuk identifikasi. Aturan keputusan berdasarkan voting tertimbang dapat dinyatakan sebagai berikut:

$$Memutuskan\ untuk\ memihak\ pada\ kelas\ k\ jika \sum_{m=1}^{M} w_m \tilde{s}_{k,m} > \sum_{m=1}^{M} w_m \tilde{s}_{n,m} \forall n, k \neq n \quad (6.32)$$

di mana wm adalah bobot yang ditetapkan pada pencocokan ke-m. Fusi Keputusan Bayesian: Skema fusi keputusan Bayesian bergantung pada transformasi label keputusan diskret yang dikeluarkan oleh pencocok individu menjadi nilai probabilitas kontinu. Langkah pertama dalam transformasi adalah pembuatan matriks kebingungan untuk setiap pencocok dengan menerapkan pencocok ke set pelatihan D.

Pertimbangkan sistem verifikasi multibiometrik. Biarkan C^m menjadi matriks kebingungan 2 × 2 untuk pencocokan ke-m. Elemen ke-(j, k) dari matriks C^m (dilambangkan sebagai $c_{j,k}^m$) adalah jumlah instans dalam set data pelatihan di mana pola yang label kelas sebenarnya adalah ω_j ditetapkan ke kelas ω_k oleh pencocokan ke-m, di mana j, k = 0, 1. Biarkan jumlah total sampel di D menjadi L dan jumlah elemen yang termasuk dalam kelas ω_j menjadi L_j.

Misalkan $u_m \in \{0, 1\}$ adalah label kelas yang ditetapkan pada sampel uji oleh pencocok ke-m. Nilai $c_{j,u_m}^m L_j$ dapat dianggap sebagai estimasi probabilitas bersyarat $P(u_m|\omega_j)$ dan L_j/L dapat diperlakukan sebagai estimasi probabilitas prior kelas ωj. Dengan mempertimbangkan vektor keputusan yang dibuat oleh M pencocok $u = [u_1, u_2, , u_M]$, probabilitas posterior kelas ω j, yaitu, $P(\omega_j|u)$ dapat dihitung menurut aturan Bayes sebagai berikut:

$$p(\omega_j|u) = \frac{p(u|\omega_j)P(\omega_j)}{p(u)} \quad (6.33)$$

di mana j = 0, 1 dan $P(u) = \sum_{j-0}^{i} P(u|\omega_j)P(\omega_j)$. Oleh karena itu, tingkat kesalahan minimum

Aturan keputusan Bayes dapat dinyatakan sebagai

$$Memutuskan\ \omega_1\ jika\ P\ (u|\omega_1)P(\omega_1) > P(u|\omega_0)P(\omega_0) \qquad (6.34)$$

Untuk menyederhanakan perhitungan P (u|ω_j), kita dapat mengasumsikan independensi statistik antara pencocok yang berbeda. Berdasarkan asumsi ini, P (u|ω_j) adalah hasil kali probabilitas marginal, yaitu,

$$Menentukan\ \omega_1\ jika\ P(u|\omega_j) = P(u_1, u_2, \ldots u_M|\omega_j) = \prod_{m=1}^{M} P(u_m|\omega_j) \qquad (6.35)$$

Dengan asumsi independensi, aturan keputusan dikenal sebagai aturan Bayes naif, yang dapat dinyatakan sebagai

$$Menentukan\ \omega_1\ jika\ P(\omega_1)\prod_{m=1}^{M} P(u_m|\omega_1) > P(\omega_0)\prod_{m=1}^{M} P(u_m|\omega_0) \qquad (6.36)$$

Perhatikan bahwa dengan mengubah ambang batas pencocokan τm untuk pencocok biometrik ke-m, adalah mungkin untuk memvariasikan probabilitas P(u_m|ω_j) dari pencocok spesifik tersebut. Namun, dalam sistem multibiometrik, tujuannya adalah untuk meminimalkan tingkat kesalahan global (tingkat kesalahan keseluruhan dari sistem multibiometrik setelah penggabungan keputusan dari pencocok biometrik individual). Oleh karena itu, seseorang harus menemukan solusi optimal untuk ambang batas lokal {τ_1, τ_2 , τ_M} sehingga tingkat kesalahan global diminimalkan.

Sistem multibiometrik diharapkan dapat mengurangi beberapa keterbatasan sistem unibiometrik dengan mengkonsolidasikan bukti yang disajikan oleh beberapa sumber biometrik yang berbeda. Integrasi bukti dalam sistem multibiometrik dikenal sebagai fusi informasi dan, jika diterapkan dengan tepat, dapat meningkatkan akurasi pencocokan sistem pengenalan biometrik. Selain meningkatkan akurasi pencocokan, sistem multibiometrik yang dirancang dengan baik juga dapat meningkatkan cakupan populasi (yaitu, mengurangi tingkat kegagalan pendaftaran), memberikan fleksibilitas, dan mencegah aktivitas pemalsuan.

Desain sistem multibiometrik diatur oleh beberapa faktor, termasuk sumber informasi yang tersedia, urutan akuisisi dan pemrosesan yang akan diadopsi, jenis informasi yang akan digabungkan, dan strategi fusi yang akan digunakan. Sistem multibiometrik dapat memanfaatkan kekuatan pelengkap dari berbagai sumber biometrik seperti beberapa sensor, beberapa skema representasi atau fitur dan algoritma pencocokan, beberapa contoh atau sampel dari sifat biometrik yang sama, dan beberapa sifat. Secara umum, sulit untuk memprediksi sumber informasi biometrik optimal yang relevan untuk aplikasi tertentu dan metodologi fusi yang tepat berdasarkan kinerja pengenalan saja. Faktor-faktor seperti biaya penerapan sistem, waktu pemrosesan, kenyamanan pengguna, skalabilitas, dll.

Juga memainkan peran besar dalam memilih sumber informasi biometrik dan mengadopsi strategi fusi tertentu. Penggabungan informasi dalam biometrik dapat dilakukan pada beberapa tingkatan. Dalam bab ini, beberapa strategi penggabungan yang berkaitan dengan sensor, set fitur, skor kecocokan, peringkat, dan tingkat keputusan diperkenalkan. Biasanya, strategi integrasi awal (misalnya, tingkat sensor atau fitur) diharapkan menghasilkan kinerja yang lebih baik daripada strategi integrasi akhir (misalnya, tingkat skor). Namun, sulit untuk memprediksi perolehan kinerja karena masing-masing strategi ini sebelum menerapkan metodologi penggabungan tertentu. Penggabungan pada tingkat skor biasanya menawarkan keseimbangan terbaik antara konten informasi dan kemudahan penggabungan. Oleh karena itu, penggabungan tingkat skor telah diadopsi oleh beberapa sistem multibiometrik praktis. Berbagai macam teknik penggabungan tingkat skor telah diusulkan dalam literatur dan kinerja setiap skema bergantung pada jumlah dan kualitas data pelatihan yang tersedia.

Meskipun ketersediaan berbagai sumber informasi biometrik (yang berkaitan dengan satu sifat atau beberapa sifat) dapat menjadi alasan kuat untuk penggabungan, korelasi antara sumber-sumber tersebut perlu diperiksa sebelum menentukan kesesuaiannya untuk penggabungan. Menggabungkan sumber-sumber yang tidak berkorelasi atau berkorelasi negatif yang membuat kesalahan pelengkap diharapkan menghasilkan peningkatan yang lebih baik dalam kinerja pencocokan daripada menggabungkan sumber-sumber yang berkorelasi positif. Selain ketergantungan antara sumber-sumber tersebut, perbedaan kinerja antara masing-masing sumber informasi juga memengaruhi akurasi pencocokan skema penggabungan. Jika perbedaan kinerja antara pencocok komponen besar dan jika skema penggabungan gagal memperhitungkan perbedaan ini, maka kinerja pencocok yang "lebih kuat" dapat diencerkan oleh pencocok yang "lebih lemah".

Hal ini juga dapat berdampak pada keamanan sistem biometrik karena sistem dapat dielakkan dengan memalsukan modalitas yang "lebih lemah". Akhirnya, pengembangan antarmuka komputer manusia (HCI) yang tangguh diperlukan untuk memungkinkan perolehan data multibiometrik yang efisien dari individu. HCI yang mudah digunakan dapat menghasilkan pembiasaan pengguna yang cepat dan mendorong perolehan data biometrik berkualitas tinggi, sehingga mengurangi tingkat kesalahan. Dengan meningkatnya penggunaan biometrik dalam aplikasi autentikasi dan permintaan yang terus meningkat untuk akurasi pencocokan yang lebih tinggi, sistem multibiometrik sekarang sedang dipertimbangkan sebagai solusi biometrik generasi berikutnya dalam berbagai sistem pengenalan orang di pemerintahan, militer, dan komersial.

BAB 7
KEAMANAN SISTEM BIOMETRIK

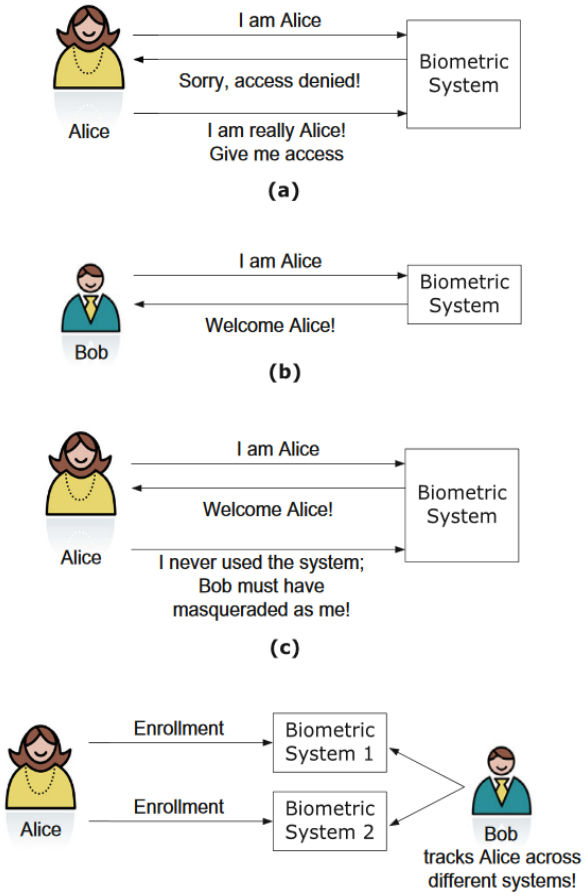
Alasan utama penggunaan pengenalan biometrik adalah untuk menangkap penjahat, mengurangi penipuan finansial, mengamankan perbatasan nasional, atau mengendalikan akses ke fasilitas fisik dan sumber daya logis. Ketika sistem biometrik gagal memenuhi tujuan ini, keamanan sistem dikatakan telah dilanggar. Pelanggaran keamanan ini dapat berupa penolakan layanan kepada pengguna yang sah, intrusi oleh pengguna yang tidak sah, klaim penolakan oleh pengguna yang sah, atau penyalahgunaan data biometrik untuk tujuan yang tidak diinginkan. Kegagalan keamanan dapat terjadi baik karena keterbatasan intrinsik sistem biometrik atau karena serangan eksplisit oleh musuh, yang mungkin orang dalam (misalnya, administrator dan pengguna yang sah) atau penyerang eksternal. Tujuan dari bab ini adalah untuk menguraikan serangan umum terhadap sistem biometrik dan membahas teknik yang dapat digunakan untuk melawannya. Secara khusus, bab ini akan berfokus pada dua serangan paling terkenal yang khusus untuk sistem biometrik, yaitu, pemalsuan ciri biometrik dan kebocoran data biometrik. Deteksi keaktifan dan algoritma keamanan templat biometrik yang dapat mengurangi dua ancaman di atas akan dibahas secara rinci.

7.1 PENDAHULUAN

Pertanyaan wajar yang muncul dalam pengenalan biometrik adalah sistem biometrik mana yang "paling" cocok untuk aplikasi tertentu. Tentu saja, jawaban untuk pertanyaan ini tidak hanya bergantung pada kelebihan dan keterbatasan teknis sistem biometrik (misalnya, akurasi dan throughput pencocokan), tetapi juga pada faktor sosial ekonomi lainnya seperti penerimaan pengguna dan biaya sistem. Namun, mengingat semua faktor lainnya sama, orang jelas lebih memilih sistem biometrik yang memiliki kemungkinan kegagalan paling kecil. Tetapi apa sebenarnya yang dimaksud dengan kegagalan sistem biometrik? Ingatlah bahwa dalam sebagian besar aplikasi, tujuan utama penggunaan biometrik adalah untuk menyediakan autentikasi yang tidak dapat disangkal. Autentikasi menyiratkan bahwa (a) hanya pengguna yang sah atau berwenang yang dapat mengakses sumber daya fisik atau logis yang dilindungi oleh sistem biometrik dan (b) penipu dicegah mengakses fasilitas atau informasi yang dilindungi. Non-repudiation memastikan bahwa individu yang mengakses sumber daya tertentu tidak dapat kemudian menyangkal menggunakannya. Dengan demikian, integritas sistem biometrik ditentukan oleh kemampuannya untuk menjamin autentikasi yang tidak dapat disangkal.

Dari sudut pandang pengguna, ada dua persyaratan tambahan yang harus dipenuhi oleh sistem biometrik. Pertama, pengguna yang sah harus memiliki akses yang tepat waktu dan andal ke sumber daya/layanan yang dilindungi. Ini disebut sebagai ketersediaan sistem biometrik. Kedua, sistem biometrik dan data pribadi yang tersimpan di dalamnya harus digunakan hanya untuk fungsi yang dimaksudkan, yaitu untuk mengendalikan akses ke

sumber daya tertentu dan bukan untuk tujuan lain yang tidak dimaksudkan. Ini dikenal sebagai persyaratan kerahasiaan. Ketika satu atau lebih dari tiga harapan di atas (integritas, ketersediaan, dan kerahasiaan) tidak terpenuhi, sistem biometrik dianggap telah gagal.Kegagalan sistem biometrik umumnya menyebabkan pelanggaran keamanan dalam aplikasi atau fasilitas yang dirancang untuk dilindungi. Ancaman keamanan dalam sistem biometrik mengacu pada kemungkinan kegagalan sistem. Bergantung pada jenis kegagalan, ancaman keamanan ini dapat diklasifikasikan ke dalam empat kelas utama (lihat Gambar 7.1).



Gambar 7.1 Empat Kelas Utama Ancaman Keamanan Dalam Sistem Biometrik. (A) Penolakan Layanan, (B) Intrusi, (C) Penolakan, Dan (D) Fungsi Merayap.

Denial-of-service (DoS) Pengguna yang sah dicegah memperoleh akses ke sistem atau sumber daya yang menjadi hak mereka, sehingga menyebabkan ketidaknyamanan bagi pengguna asli. Hal ini melanggar persyaratan ketersediaan. Denial-of-service yang sering terjadi kemungkinan besar pada akhirnya akan mendorong pengguna untuk meninggalkan sistem biometrik sama sekali.

1. Intrusi: Pengguna yang tidak sah memperoleh akses tidak sah ke sistem. Karena intrusi memengaruhi integritas dasar sistem biometrik, hal ini umumnya dianggap sebagai ancaman keamanan yang paling serius.
2. Penolakan: Pengguna yang sah menyangkal penggunaan sistem setelah mengaksesnya. Pengguna yang korup dapat menyangkal tindakan mereka dengan

mengklaim bahwa pengguna yang tidak sah dapat menyusup ke sistem menggunakan identitas mereka.

3. Perambahan fungsi: Seorang penyerang mengeksploitasi sistem biometrik yang dirancang untuk menyediakan kontrol akses ke sumber daya tertentu untuk melayani aplikasi lain, yang tidak pernah dimaksudkan untuk dilakukan oleh sistem. Misalnya, templat sidik jari yang diperoleh dari basis data bank dapat digunakan untuk mencari catatan kesehatan orang tersebut dalam basis data medis. Hal ini melanggar persyaratan kerahasiaan. Meskipun masalah perambatan fungsi telah diajukan terutama sebagai ancaman keamanan, hal itu juga secara luas dianggap sebagai ancaman besar terhadap privasi pengguna.

Kepercayaan publik dan penerimaan teknologi biometrik akan bergantung pada kemampuan perancang sistem untuk melindungi dari semua kemungkinan ancaman keamanan. Namun, tidak ada sistem yang mungkin benar-benar aman dan anti-gagal. Dengan keadaan yang tepat dan banyak waktu serta sumber daya, sistem keamanan apa pun dapat dibobol. Meskipun perancang sistem biometrik harus berusaha untuk menutup sebanyak mungkin celah, kenyataannya adalah bahwa tingkat keamanan yang dipastikan umumnya didasarkan pada persyaratan aplikasi. Dengan kata lain, tingkat keamanan dalam sistem biometrik yang digunakan untuk aplikasi penting seperti kontrol perbatasan dapat diharapkan jauh lebih tinggi daripada sistem biometrik yang digunakan untuk masuk ke komputer pribadi.

Langkah pertama dalam menganalisis keamanan sistem biometrik adalah mendefinisikan model ancaman, yang mengidentifikasi berbagai agen ancaman dan serangan. Secara umum, agen ancaman dapat didefinisikan sebagai orang atau benda yang dapat atau memiliki kekuatan untuk menggagalkan operasi sistem yang dimaksudkan. Dalam konteks sistem biometrik, ada dua jenis agen ancaman.

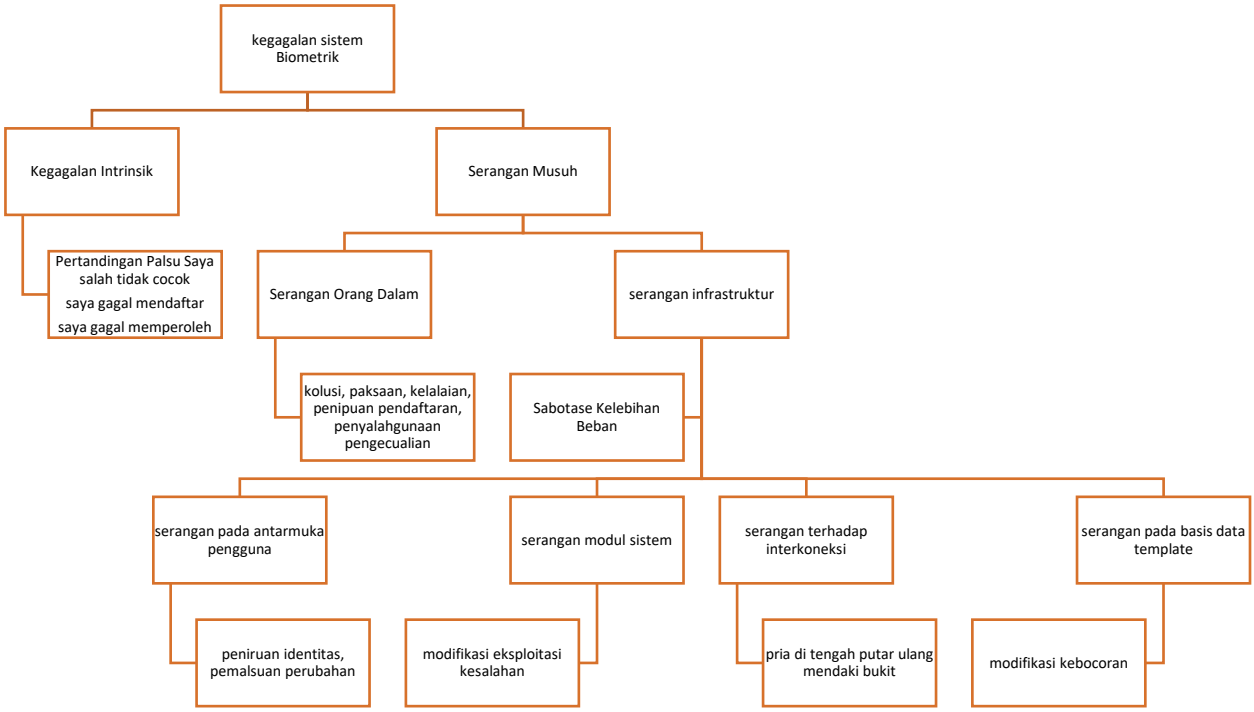
Keterbatasan intrinsik: Bahkan jika tidak ada serangan eksternal, sistem biometrik dapat gagal karena keterbatasan intrinsiknya. Seperti yang dibahas dalam Bab 1, semua sistem biometrik rentan terhadap dua jenis kesalahan, yaitu, pencocokan palsu dan ketidakcocokan palsu. Selain itu, perangkat biometrik juga dapat gagal menangkap atau memperoleh sampel pengenal biometrik yang diberikan kepadanya oleh pengguna, yang menyebabkan kegagalan pendaftaran dan kegagalan menangkap kesalahan. Karena kesalahan ini disebabkan karena keterbatasan intrinsik berbagai modul dalam sistem biometrik seperti sensor, ekstraktor fitur, dan pencocok, dan bukan oleh serangan yang disengaja, kegagalan atau pelanggaran keamanan yang dihasilkan dikenal sebagai serangan tanpa upaya.

Musuh: Sistem biometrik juga dapat gagal karena manipulasi oleh musuh, yang dapat berupa orang dalam atau entitas eksternal. Orang dalam adalah pengguna resmi sistem biometrik, yang mencakup administrator sistem (pengguna super) dan orang lain yang terdaftar dalam sistem biometrik. Entitas eksternal dapat diklasifikasikan sebagai penipu dan penyerang. Sementara istilah penipu mengacu pada setiap individu yang secara sengaja atau tidak sengaja mencoba menyamar sebagai orang lain yang terdaftar, penyerang adalah orang yang mencoba merusak pengoperasian sistem biometrik.

Serangan mengacu pada mekanisme atau jalur aktual yang dapat digunakan untuk menghindari sistem biometrik. Taksonomi serangan yang dapat dilakukan terhadap sistem biometrik ditunjukkan pada Gambar 7.2. Berdasarkan agen ancaman yang digunakan dalam serangan, mekanisme serangan dapat dikategorikan secara luas sebagai yang disebabkan oleh keterbatasan intrinsik (serangan tanpa upaya) dan yang disebabkan oleh musuh.Konsekuensi dari serangan tanpa upaya akan bergantung pada aplikasi.

Misalnya, dalam sistem verifikasi biometrik, kesalahan ketidakcocokan yang salah akan menyebabkan penolakan layanan dan ketidaknyamanan bagi pengguna asli. Di sisi lain, dalam aplikasi pengenalan negatif seperti penyaringan, ketidakcocokan palsu akan menyebabkan intrusi dan kecocokan palsu akan menyebabkan penolakan layanan. Karena kegagalan untuk mendaftarkan dan kegagalan untuk menangkap kesalahan mengharuskan operator untuk kembali pada mekanisme autentikasi tradisional (yang mungkin tidak dapat diandalkan) seperti kartu identitas, efek dari kesalahan ini mirip dengan ketidakcocokan palsu. Keterbatasan intrinsik sistem biometrik juga membuatnya sulit untuk bertahan terhadap klaim penolakan.

Probabilitas keberhasilan serangan tanpa upaya terkait dengan kinerja pengenalan sistem biometrik. Berbagai metrik untuk mengukur kinerja pengenalan sistem biometrik telah dibahas dalam Bab 1. Metrik ini meliputi rasio kecocokan palsu (FMR), rasio ketidakcocokan palsu (FNMR), rasio kegagalan untuk mendaftarkan (FTER), rasio kegagalan untuk menangkap (FTCR), rasio identifikasi positif palsu (FPIR), dan rasio identifikasi negatif palsu (FNIR). Kinerja pengenalan berbagai sistem biometrik juga telah dibahas secara rinci dalam bab 2-6. Karena kinerja pengenalan sangat penting bagi penerimaan publik terhadap sistem biometrik, ada dorongan konstan dalam komunitas penelitian untuk mengembangkan sensor baru, representasi yang kuat, dan skema pencocokan yang efektif untuk meningkatkan kinerja pengenalan sistem biometrik.



Gambar. 7.2 Taksonomi Serangan Yang Dapat Dilakukan Terhadap Sistem Biometrik.

Dalam bab ini, fokusnya adalah pada serangan yang dapat dilakukan oleh musuh. Tidak seperti kasus serangan tanpa upaya, kemungkinan keberhasilan serangan musuh bergantung pada sejumlah faktor nyata maupun tidak nyata. Ini termasuk detail implementasi dan operasional sistem biometrik, bagaimana sistem biometrik terintegrasi dengan aplikasi keseluruhan (misalnya, bagaimana autentikasi biometrik berinteraksi dengan modul lain dalam aplikasi kontrol akses fisik), sumber daya musuh (misalnya, waktu yang tersedia dan daya komputasi), dan perilaku pengguna yang berinteraksi dengan sistem biometrik. Oleh karena itu, relatif sulit untuk memprediksi terlebih dahulu semua kemungkinan cara sistem biometrik dapat diserang. Hanya mekanisme serangan yang umum ditemui dan berbagai tindakan pencegahan yang dapat diterapkan untuk melindungi sistem biometrik terhadap ancaman keamanan yang dihasilkan yang dipertimbangkan dalam bagian di bawah ini.

7.2 SERANGAN MUSUH

Seorang musuh yang bermaksud merusak sistem biometrik dapat memanfaatkan kerentanan baik pada elemen manusia maupun pada infrastruktur sistem. Dengan demikian, serangan musuh dapat dikategorikan sebagai serangan orang dalam dan serangan infrastruktur seperti yang ditunjukkan pada Gambar 7.2. Penting untuk ditekankan bahwa istilah "serangan orang dalam" tidak hanya mencakup kasus-kasus ketika pengguna yang sah

sendiri berubah menjadi jahat dan dengan sengaja merusak sistem biometrik, tetapi juga mencakup kasus-kasus ketika musuh eksternal menghindari sistem biometrik melalui keterlibatan langsung atau tidak langsung dari orang dalam.

Serangan Orang Dalam

Sistem biometrik memerlukan interaksi manusia pada sejumlah tahap. Misalnya, administrator manusia biasanya diminta untuk melakukan pendaftaran dan pembatalan pendaftaran pengguna. Selain itu, administrator juga dapat terlibat dalam penyesuaian parameter keamanan yang mengendalikan kinerja sistem biometrik seperti ambang batas pada skor kecocokan dan batas minimum pada kualitas sampel biometrik yang diperoleh. Dalam aplikasi yang diawasi, administrator juga menunjuk operator untuk mengawasi berfungsinya sistem biometrik dengan baik dan membimbing pengguna. Operator juga biasanya bertanggung jawab atas pengoperasian sistem cadangan yang akan digunakan jika sistem biometrik tidak tersedia atau ketika terjadi kegagalan pendaftaran/pengambilan kesalahan. Terakhir, ada pengguna reguler yang mengakses aplikasi atau sumber daya setelah mengautentikasi diri mereka sendiri menggunakan sistem biometrik. Interaksi manusia ini dapat dimanfaatkan dengan lima cara berikut untuk melanggar keamanan sistem biometrik.

1. **Kolusi**: Ini merujuk pada skenario di mana pengguna yang sah dengan sengaja berubah menjadi jahat dan menyerang sistem biometrik baik secara individu maupun bekerja sama dengan musuh eksternal (mungkin sebagai imbalan atas keuntungan moneter). Serangan semacam itu dapat menyebabkan pelanggaran keamanan yang serius, terutama jika penyerang adalah administrator sistem. Karena administrator biasanya berstatus sebagai pengguna super dengan kewenangan untuk mengubah atau mengendalikan sebagian besar modul sistem biometrik, akan sangat sulit untuk melindungi diri dari serangan ini. Bahkan pengguna biasa dapat berkolusi dengan musuh untuk melanggar keamanan. Misalnya, pengguna yang jahat dapat memfasilitasi akses tidak sah (misalnya, membuka pintu dalam aplikasi kontrol akses fisik) kepada penyerang dengan menunjukkan ciri biometriknya sendiri. Satu-satunya perlindungan terhadap serangan semacam itu adalah dengan menegakkan perilaku yang bertanggung jawab di antara pengguna yang sah melalui pelatihan yang tepat, pemantauan yang ketat, dan audit semua transaksi autentikasi untuk mendeteksi pola aktivitas yang tidak biasa, dan menghukum mereka yang tidak mematuhi aturan. Paksaan: Serangan paksaan mirip dengan kolusi, satu-satunya perbedaan adalah bahwa pengguna yang dipaksa tidak melakukan serangan dengan sukarela. Sebaliknya, pengguna yang berwenang dipaksa untuk menjadi jahat, mungkin melalui ancaman fisik (misalnya, dengan todongan senjata) atau pemerasan. Sebaiknya, deteksi kejadian paksaan dilakukan secara andal tanpa menempatkan pengguna asli pada risiko yang lebih besar dari musuh.
2. **Kelalaian**: Penyerang eksternal juga dapat memanfaatkan kelalaian pengguna yang berwenang untuk menghindari sistem biometrik. Contoh tipikal adalah kegagalan pengguna yang berwenang untuk keluar dari sistem dengan benar setelah

menyelesaikan transaksi mereka. Membuka pintu atau mengizinkan tailgating dalam skenario kontrol akses fisik juga dapat dianggap sebagai kelalaian, jika niat pengguna yang berwenang tidak jahat. Kelalaian dapat diminimalkan dengan melatih pengguna yang berwenang secara berkala dan terus-menerus mengingatkan mereka tentang pedoman yang harus diikuti.

3. **Penipuan Pendaftaran**: Penyerang dapat mendaftarkan dirinya ke dalam sistem biometrik secara ilegal (dengan identitas palsu) dengan membuat ciri-ciri biometriknya beserta kredensial palsu (misalnya, paspor dan akta kelahiran palsu). Alasan untuk memasukkan kerentanan ini ke dalam serangan orang dalam adalah karena hal ini terutama disebabkan oleh cacat dalam desain sistem biometrik, yaitu ketergantungan yang berlebihan pada sistem manajemen identitas yang ada (lama) untuk pendaftaran. Dalam beberapa aplikasi biometrik, seperti memverifikasi pemegang tiket, identitas asli orang tersebut tidak menjadi masalah selama dia adalah orang yang membayar tiket tersebut. Namun, dalam banyak aplikasi pemerintah, seperti penyaluran dana kesejahteraan, pendaftaran yang curang dapat menjadi masalah serius. Solusi untuk mencegah penipuan pendaftaran adalah dengan mencocokkan ciri-ciri biometrik pengguna baru dengan ciri-ciri semua pengguna yang terdaftar untuk mendeteksi identitas duplikat bahkan sebelum pengguna baru ditambahkan ke dalam sistem. Proses ini disebut deduplikasi, yang merupakan masalah yang menantang karena jumlah pengguna yang terdaftar bisa sangat besar. Misalnya, ada lebih dari 75 juta pelancong yang terdaftar dalam sistem US-VISIT dan sekitar 600 juta orang diperkirakan akan terdaftar di bawah proyek Identitas Unik India selama kurun waktu lima tahun ke depan. Deduplikasi dalam aplikasi skala besar tersebut memerlukan sumber daya komputasi yang besar serta sistem biometrik dengan tingkat identifikasi positif palsu dan negatif palsu yang sangat rendah (FRIR dan FNIR). Jika deduplikasi diabaikan karena pertimbangan praktis seperti kebutuhan untuk segera beralih dari sistem manajemen identitas lama ke sistem berbasis biometrik, hal itu pasti akan memengaruhi integritas sistem biometrik yang dihasilkan.
4. **Penyalahgunaan Pengecualian**: Sebagian besar sistem biometrik dilengkapi dengan mekanisme fall-back untuk memungkinkan penanganan situasi luar biasa yang dapat menyebabkan penolakan layanan kepada pengguna yang sah. Contoh skenario pengecualian dapat mencakup pemrosesan pengguna tanpa jari dalam sistem pengenalan berbasis sidik jari dan kegagalan beberapa komponen perangkat keras/perangkat lunak dari sistem biometrik. Dalam kasus seperti itu, administrator sistem memiliki kemampuan untuk melewati sistem pengenalan dan membuat keputusan berdasarkan kredensial lain seperti rahasia dan token. Hal ini memberikan motivasi bagi penyerang untuk memicu prosedur pemrosesan pengecualian (misalnya, dengan sengaja menurunkan kualitas sifat biometriknya) dan mencoba mengeksploitasi celah dalam mekanisme fall-back. Masalah tersebut dapat

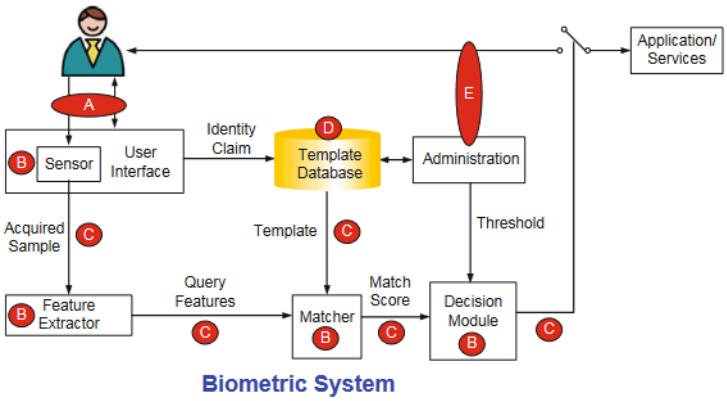
diminimalkan dengan meningkatkan keandalan sistem biometrik dan menggunakan beberapa modalitas biometrik untuk memperluas cakupan populasi.

Serangan Infrastruktur

Sistem biometrik generik terdiri dari modul-modul fungsional seperti sensor, ekstraktor fitur, basis data templat, pencocok, dan modul keputusan. Modul-modul fungsional ini pada gilirannya terdiri dari komponen perangkat keras dan perangkat lunak, dan bersama-sama dengan saluran komunikasi yang menghubungkannya, mereka membentuk infrastruktur sistem biometrik. Namun, penting untuk menyadari bahwa ada keragaman besar dalam konfigurasi fisik sistem biometrik. Misalnya, dimungkinkan untuk menempatkan semua modul fungsional dan antarmuka di antara mereka pada satu kartu pintar (atau lebih umum prosesor yang aman). Dalam sistem seperti itu, yang dikenal sebagai teknologi sistem-pada-kartu atau pencocokan-pada-kartu, informasi biometrik tidak pernah meninggalkan kartu (atau chip) dan hanya hasil pengenalan (cocok atau tidak cocok) yang dikirimkan ke aplikasi. Di sisi lain, pertimbangkan Sistem Identifikasi Sidik Jari Otomatis (AFIS) yang digunakan dalam aplikasi forensik. Dalam skenario AFIS, modul sistem biometrik biasanya didistribusikan di berbagai lokasi fisik (misalnya sensor mungkin berada di tempat kejadian perkara, ekstraktor fitur dan modul keputusan mungkin berada di kantor investigasi regional, dan pencocokan dan basis data di pusat regional atau nasional). Konfigurasi perantara lainnya di mana sensor dan ekstraktor fitur mungkin berada bersama di lokasi terpencil (misalnya, telepon seluler), sementara pencocokan dan basis data berada di server juga dimungkinkan.

Ada sejumlah cara yang dapat dilakukan penyerang untuk memanipulasi infrastruktur biometrik yang menyebabkan pelanggaran keamanan. Serangan yang umum terjadi pada sistem keamanan seperti sabotase dan kelebihan muatan juga dapat dilakukan terhadap sistem biometrik. Sabotase biasanya melibatkan kerusakan fisik pada satu atau beberapa komponen infrastruktur sehingga seluruh sistem biometrik menjadi tidak berguna. Contoh sabotase termasuk menonaktifkan catu daya, merusak permukaan sensor, atau menimbulkan gangguan berlebihan (interferensi) yang mencegah pengoperasian normal sistem. Kelebihan muatan adalah upaya untuk mengalahkan sistem dengan membanjirinya dengan permintaan autentikasi. Motivasi untuk serangan ini biasanya adalah untuk menolak akses ke pengguna asli. Namun, hal itu juga dapat digunakan sebagai taktik untuk memaksa operator mengandalkan mekanisme fall-back yang mungkin lebih mudah dielakkan.

Serangan infrastruktur lainnya dapat dipelajari secara sistematis dengan mengkategorikannya (lihat Gambar 7.3) berdasarkan titik serangan dan sifat serangan. Empat kategori berikut dapat diidentifikasi: (a) serangan pada antarmuka antara pengguna dan sistem biometrik, (b) serangan pada modul sistem (sensor, ekstraktor fitur, pencocok, dan modul keputusan), (c) serangan pada interkoneksi antara modul, dan (d) serangan pada basis data templat.



Gambar 7.3 Jenis Serangan Musuh Dalam Sistem Biometrik.

Lima area kerentanan utama adalah:

(a) Antarmuka sistem biometrik pengguna,
(b) Modul sistem biometrik,
(c) Interkoneksi antara modul biometrik,
(d) Basis data templat, dan
(e) Serangan melalui orang dalam (administrator atau pengguna terdaftar).

7.3 SERANGAN PADA ANTARMUKA PENGGUNA

Secara umum, setiap upaya penyerang untuk membobol sistem dengan menampilkan ciri biometrik dapat dianggap sebagai serangan pada tingkat antarmuka pengguna. Pada tingkat ini, serangan dan tindakan pencegahan berikut dapat dilakukan.

Peniruan Identitas

Hal ini mengacu pada situasi saat penipu mencoba menyusup ke sistem dengan menyamar sebagai pengguna resmi lainnya. Peniruan identitas dapat dilakukan secara kasual atau tertarget. Dalam peniruan identitas kasual, identitas yang akan diserang dipilih secara acak dan penipu tidak mengubah pengenal biometriknya sendiri dengan cara apa pun. Probabilitas keberhasilan dalam serangan semacam itu biasanya diukur dengan rasio kecocokan palsu (FMR) dari sistem biometrik. Serangan ini dapat dilawan dengan memilih nilai FMR yang sangat rendah dan dengan membatasi jumlah upaya kegagalan yang diizinkan dalam jangka waktu tertentu. Peniruan identitas yang ditargetkan terjadi ketika penipu menyerang identitas tertentu yang tercantum dalam sistem biometrik, yang diketahui lebih mudah ditiru (juga dikenal sebagai "domba" di Kebun Binatang Doddington). Serangan ini mengeksploitasi fakta bahwa FMR tidak seragam di antara semua pengguna. Penipu juga dapat menargetkan identitas yang karakteristik biometriknya diketahui mirip dengan sifatnya (juga dikenal sebagai serangan "Kembaran Jahat"). Tindakan pencegahan yang sama yang digunakan terhadap peniruan identitas kasual dapat digunakan untuk membatasi keberhasilan jenis serangan ini.

Terakhir, penipu juga dapat mengubah karakteristik biometriknya agar sesuai dengan identitas yang diserang. Nama umum untuk serangan semacam itu adalah mimikri. Contoh serangan ini termasuk mengubah suara seseorang, memalsukan tanda tangan (lihat Gambar

7.4), atau meniru pola gaya berjalan. Ancaman ini lebih umum dalam sistem yang menggunakan sifat biometrik perilaku dan dalam aplikasi dengan mode operasi tanpa pengawasan. Untuk menangkal serangan ini diperlukan sistem biometrik yang memiliki tingkat kecocokan palsu (FMR) yang rendah dengan pemalsuan yang terampil.

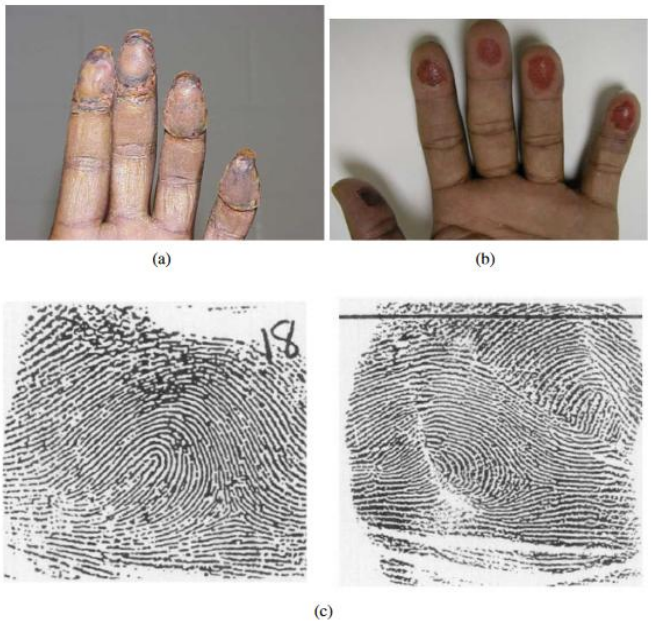
Gambar 7.4 Contoh Serangan Mimikri

(a) Contoh tanda tangan asli seseorang,
(b) Pemalsuan tanda tangan pada (a) yang dilakukan oleh penipu.

Pengaburan

Setiap upaya yang disengaja oleh penyerang untuk mengubah karakteristik biometriknya agar tidak terdeteksi oleh sistem biometrik disebut pengaburan. Jadi, perbedaan utama antara mimikri dan pengaburan adalah motivasi di balik serangan tersebut. Pengaburan terutama berlaku dalam aplikasi pengenalan negatif, di mana penyerang ingin menyembunyikan identitas aslinya. Namun, pengaburan juga dapat berlaku dalam sistem verifikasi yang menggunakan mekanisme fall-back untuk menangani penolakan palsu. Dalam skenario ini, penyerang dapat mencoba melewati sistem biometrik dengan memaksakan keputusan penolakan palsu dan kemudian memanfaatkan celah dalam mekanisme fall-back, yang mungkin lebih mudah dielakkan.

Pengaburan dapat dilakukan dengan sejumlah cara berbeda. Salah satu kemungkinannya adalah dengan sengaja menampilkan gambar berkualitas buruk atau sampel biometrik yang berisik (misalnya, wajah dengan ekspresi tidak netral atau mata yang sebagian terbuka) yang mungkin tidak cocok dengan templatnya dalam basis data. Dalam hal pengenalan wajah, penggunaan tata rias, rambut wajah, dan kacamata juga dapat menyebabkan ketidakcocokan palsu. Sidik jari dapat dihapus melalui teknik seperti abrasi, pemotongan, dan pembakaran, atau bahkan dapat diubah atau didistorsi melalui pembedahan (lihat Gambar 7.5). Demikian pula, wajah dapat diubah menggunakan operasi plastik dan transplantasi iris telah digambarkan dalam fiksi ilmiah populer (misalnya, dalam film Minority Report). Pengetahuan tentang detail algoritma pemrosesan biometrik dapat lebih memudahkan serangan tersebut. Misalnya, jika penyerang mengetahui bahwa sistem pengenalan wajah tertentu tidak kuat terhadap variasi pose, ia dapat dengan mudah menghindarinya dengan hanya menampilkan tampilan profil wajah.



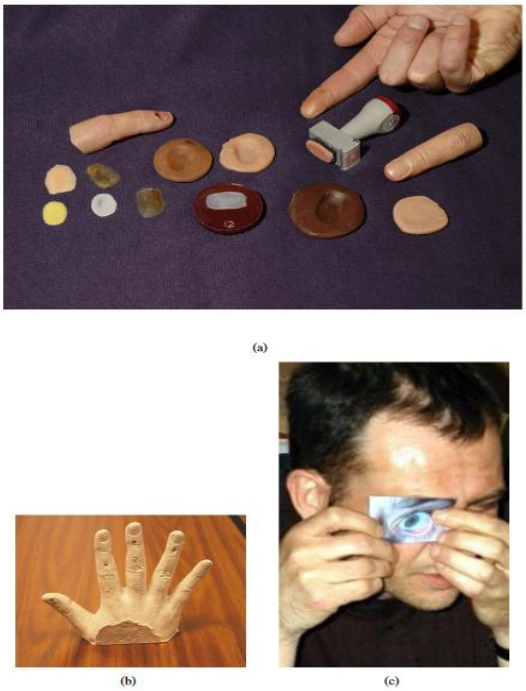
Gambar 7.5 Contoh Perubahan Sidik jari

a) Sidik jari yang ditransplantasikan dari pola tonjolan gesekan yang ditemukan di telapak kaki.
b) Sidik jari dihilangkan dengan menggigit kulit jari, dan
c) Sidik jari diubah dengan membuat potongan berbentuk Z di ujung jari, mengangkat dan menukar kedua segitiga, dan menjahitnya kembali; gambar kiri menunjukkan sidik jari asli dan sidik jari yang diubah ditunjukkan di sebelah kanan.

Solusi paling efektif terhadap pengaburan adalah meningkatkan ketahanan algoritma biometrik terhadap variasi intra-pengguna untuk mencapai tingkat ketidakcocokan palsu (FNMR) yang sangat rendah. Mungkin juga memungkinkan untuk secara otomatis mendeteksi beberapa perubahan seperti wajah yang tidak menghadap depan atau sidik jari yang dimodifikasi secara bedah dan menjadikan pengguna tersebut sebagai objek pemeriksaan sekunder.

Pemalsuan

Ini adalah serangan yang paling terkenal di tingkat antarmuka pengguna, dan melibatkan penyajian ciri biometrik palsu. Pemalsuan didefinisikan sebagai biometrik palsu yang tidak diperoleh dari orang yang hidup (lihat Gambar 7.6). Pemalsuan mencakup penyajian ciri palsu atau buatan (misalnya, jari bergetah, lapisan tipis di atas jari, foto atau topeng wajah, rekaman suara, dll.) dan hal-hal yang menyeramkan seperti bagian tubuh yang terpotong-potong (misalnya, jari yang terpotong-potong) milik pengguna yang sah ke sistem pengenalan. Jika sensor tidak dapat membedakan antara ciri biometrik palsu dan asli, penyerang dapat dengan mudah menyusup ke sistem dengan identitas palsu.



Contoh 7.6 Contoh Ciri Biometric Palsu

a) Sidik Jari Palsu Yang Terbuat Dari Lem Dan Jari Yang Dipotong-Potong.

b) Tangan Palsu Yang Terbuat Dari Plester, Dan

c) *Foto Iris*

Serangan ini memerlukan pengetahuan tentang ciri biometrik yang sesuai dengan identitas yang akan diserang. Pengetahuan ini dapat diperoleh dengan salah satu dari empat cara berikut:

(a) Berkolusi langsung dengan atau memaksa pengguna yang berwenang,

(b) Akuisisi rahasia (misalnya, mengangkat jejak sidik jari yang tersisa secara diam-diam dari sensor atau permukaan apa pun yang disentuh oleh pengguna yang berwenang, merekam suara pengguna, atau mengambil foto wajah pengguna),

(c) Memperkirakan perkiraan yang mendekati dari templat biometrik pengguna melalui serangan brute-force atau hill-climbing, dan

(d) Mencuri templat biometrik dari basis data dan merekayasa balik templat tersebut.

Sementara sistem autentikasi berbasis kata sandi tradisional bekerja dengan asumsi kerahasiaan (yaitu, hanya pengguna yang sah yang mengetahui kata sandinya), asumsi seperti itu umumnya tidak diperlukan agar sistem biometrik dapat berfungsi. Sebaliknya, kekuatan autentikasi biometrik berasal dari fakta bahwa karakteristik biometrik terhubung dengan pengguna secara fisik. Meskipun penyerang dapat memperoleh pola sidik jari pengguna yang sah, tidak akan banyak gunanya bagi penyerang jika sensor dapat memastikan bahwa sidik jari yang dipindai berasal langsung dari jari pengguna yang masih hidup. Oleh karena itu, solusi untuk melawan serangan spoof adalah dengan menggabungkan kemampuan deteksi keaktifan dalam sensor biometrik.

Perubahan yang ditunjukkan pada (c) melibatkan seorang pria yang menggunakan nama Alexander Guzman, yang ditangkap oleh petugas Florida pada tahun 1995 karena memiliki

paspor palsu dan ditemukan memiliki sidik jari yang dimutilasi. Setelah pencarian selama dua minggu berdasarkan rekonstruksi sidik jari yang diubah secara manual dan pencarian di basis data FBI, sidik jari Alexander Guzman yang direkonstruksi dikaitkan dengan sidik jari Jose Izquiredo, seorang penjahat narkoba yang melarikan diri. Contoh ini menggambarkan kegunaan sistem biometrik serta tindakan nekat yang sering dilakukan penjahat untuk menghindari sistem biometrik.

Penanggulangan: Deteksi Spoof

Deteksi spoof secara umum dapat didefinisikan sebagai pembedaan ciri biometrik nyata yang ditunjukkan oleh orang yang hidup dari ciri biometrik yang ditunjukkan melalui sumber lain. Deteksi spoof biasanya melibatkan pemeriksaan tanda-tanda vitalitas atau keaktifan manusia (misalnya, denyut nadi), suatu proses yang dikenal sebagai deteksi keaktifan. Meskipun ada perbedaan kecil antara deteksi spoof dan deteksi keaktifan, kedua istilah tersebut umumnya digunakan secara bergantian dalam literatur biometrik, yang juga merupakan kasus dalam buku ini. Deteksi spoof dapat dipisahkan dari atau diintegrasikan ke dalam proses pengenalan biometrik. Dalam sistem yang dipisahkan, tidak ada data biometrik yang diperoleh hingga sistem deteksi spoof yakin bahwa ciri biometrik tersebut ditunjukkan oleh pengguna manusia yang hidup. Di sisi lain, sistem terintegrasi mendeteksi spoof saat memproses informasi biometrik yang diperoleh (baik sebelum atau selama ekstraksi fitur). Kerentanan sistem biometrik terhadap serangan tipuan bergantung pada modalitas biometrik dan sensor khusus yang digunakan untuk menangkap ciri biometrik. Misalnya, foto dua dimensi wajah manusia mungkin cukup untuk mengelabui kamera yang digunakan dalam sistem pengenalan wajah. Namun, biasanya sangat sulit untuk menghindari sensor sidik jari optik atau kapasitif dengan menggunakan reproduksi sidik jari 2-D karena sensor tersebut secara inheren bergantung pada penangkapan variasi 3-D dalam struktur punggungan-lembah.

Meskipun deteksi tipuan sangat penting untuk memastikan integritas sistem biometrik, deteksi tipuan juga memiliki beberapa kelemahan. Pertama, hampir semua solusi deteksi tipuan meningkatkan biaya sistem biometrik. Hal ini dikarenakan kebutuhan untuk memiliki perangkat keras tambahan untuk menangkap informasi baru (misalnya, sifat spektral atau termal) atau modul perangkat lunak untuk memproses data biometrik yang telah dikumpulkan dan membedakan antara tipuan dan sifat hidup. Pemrosesan tambahan ini juga meningkatkan waktu akuisisi biometrik, sehingga mengurangi hasil sistem biometrik. Terakhir, seperti sistem biometrik yang jarang sempurna, sistem deteksi tipuan juga rentan terhadap kesalahan. Sementara sistem deteksi tipuan dapat mengidentifikasi dan menggagalkan sebagian besar upaya pemalsuan, sistem tersebut juga dapat secara tidak tepat mengklasifikasikan beberapa sifat biometrik nyata sebagai tipuan, yang menyebabkan peningkatan tingkat kegagalan penangkapan.

Meskipun ada sejumlah algoritma deteksi tipuan biometrik, algoritma tersebut dapat diklasifikasikan ke dalam tiga kelompok utama berdasarkan mekanisme yang digunakan untuk menggagalkan upaya tipuan. Pendekatan pertama melibatkan pengukuran sifat fisiologis orang yang hidup, yang meliputi denyut nadi/tekanan darah, keringat, sifat

spektral/optik kulit/jaringan manusia, karakteristik listrik/termal, dan deformasi otot/kulit. Pendekatan kedua didasarkan pada identifikasi tindakan perilaku manusia yang disengaja atau tidak disengaja seperti fluktuasi ukuran pupil, kedipan mata, dan gerakan pupil/mata/kepala/tubuh. Kategori ketiga dikenal sebagai mekanisme tantangan-respons, di mana sistem menyajikan tantangan kepada pengguna dan mengukur apakah pengguna menanggapi tantangan tersebut dengan benar. Contoh tantangan termasuk meminta pengguna untuk melafalkan frasa/teks yang dibuat secara acak, meminta pengguna untuk mengubah ekspresi wajahnya (misalnya, tersenyum atau cemberut), dan meminta pengguna untuk menyajikan beberapa ciri biometrik dalam urutan yang dibuat secara acak. Karena dua pendekatan terakhir cukup mudah untuk dibayangkan dan diterapkan, hanya pendekatan pertama yang akan dibahas secara rinci.

Deteksi Spoof Berdasarkan Sifat Fisiologis

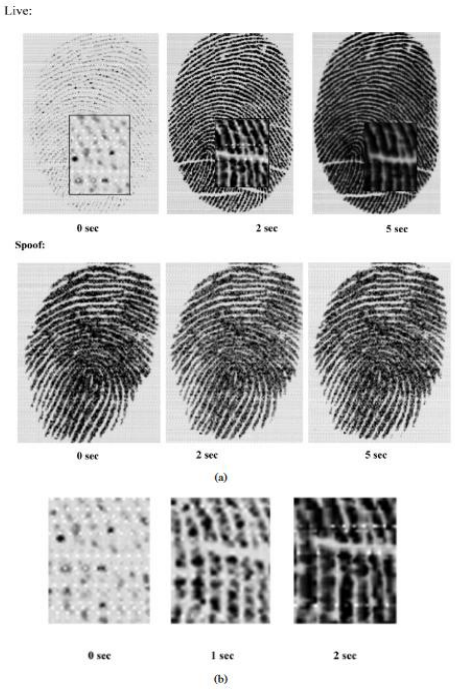
Sementara sistem biometrik didasarkan pada karakteristik fisiologis yang unik untuk setiap individu (misalnya, sidik jari, iris, wajah), algoritma deteksi spoof cenderung menggunakan karakteristik yang dapat dengan mudah membedakan tubuh manusia dari bahan bawaan (misalnya, gel silikon untuk sidik jari) yang digunakan untuk spoofing. Beberapa sifat fisiologis yang telah digunakan untuk deteksi spoof dibahas di bawah ini.

Denyut nadi/Tekanan darah

Properti ini umumnya berlaku untuk ciri biometrik seperti sidik jari dan telapak tangan yang mengharuskan pengguna untuk melakukan kontak fisik dengan sensor. Sementara denyut nadi merupakan tanda vitalitas yang baik, perangkat keras khusus mungkin diperlukan untuk merekam sifat ini. Selain itu, denyut nadi dan tekanan darah bervariasi secara signifikan dari satu orang ke orang lain dan juga dalam orang yang sama tergantung pada aktivitas fisik dan keadaan emosionalnya pada saat akuisisi. Lebih jauh lagi, pengukuran denyut nadi tunggal dapat memakan waktu hingga lima detik. Terakhir, jika karet silikon tipis direkatkan pada jari asli, detak jantung jari yang mendasarinya akan menghasilkan deteksi denyut nadi.

Keringat

Keringat mengacu pada proses berkeringat pada jari yang hidup. Jari yang hidup menunjukkan keringat selama jangka waktu tertentu sedangkan jari palsu tidak akan menunjukkan proses berkeringat. Fenomena keringat dimulai pada pori-pori keringat pada sidik jari dan menyebar di sepanjang garis tonjolan, sedangkan lembah tidak berubah. Karena proses berkeringat pada jari yang hidup, daerah di sekitar pori-pori keringat dapat terlihat membesar seiring waktu dalam serangkaian gambar sidik jari (lihat Gambar 7.7). Salah satu keterbatasan prosedur ini untuk mendeteksi jari palsu adalah bahwa untuk mengamati proses berkeringat, jari perlu tetap berada pada pemindai sidik jari selama beberapa detik. Metode berbasis keringat juga diperkirakan memiliki kesulitan dalam menangani berbagai jumlah kadar air yang terjadi pada jari manusia yang hidup.



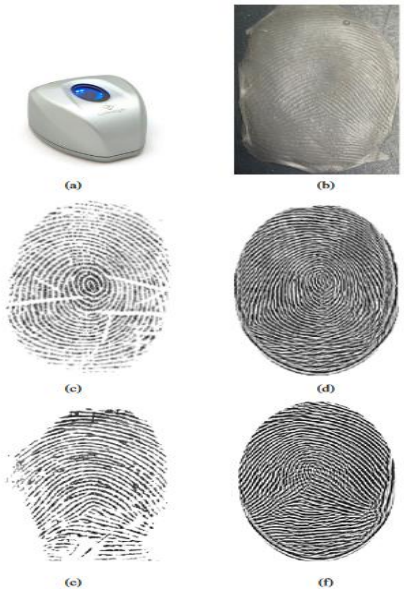
Gambar 7.7 Contoh Deteksi Spoof Sidik Jari Berdasarkan Pola Keringat Dari Jari Hidup

a) *Contoh gambar sidik jari yang diperoleh dari jari hidup (baris atas) dan jari palsu (baris bawah) yang diperoleh pada 0, 2, dan 5 detik setelah jari diletakkan pada sensor,*
b) *Urutan gambar sidik jari yang diperbesar yang menunjukkan perkembangan pola keringat dari waktu ke waktu pada jari hidup.*

Sifat spektral/optik kulit manusia

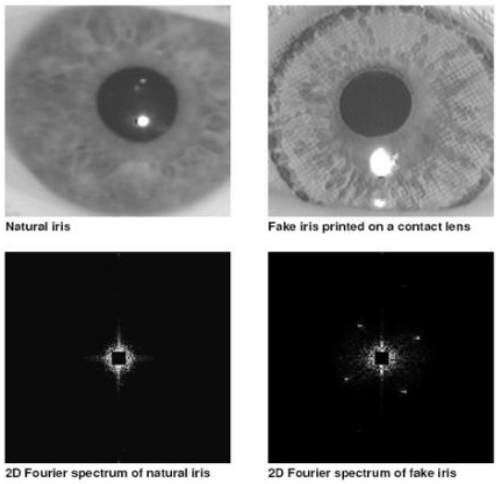
Ini adalah salah satu karakteristik paling umum yang telah berhasil digunakan untuk deteksi spoof dalam banyak sistem biometrik, termasuk sidik jari, telapak tangan, wajah, dan iris. Sifat optik yang dapat diukur meliputi sifat penyerapan, refleksi, hamburan, dan refraksi dalam kondisi pencahayaan yang berbeda (seperti panjang gelombang, polarisasi, koherensi). Dalam kasus sidik jari, analisis multispektral dapat digunakan untuk mengukur sifat permukaan serta sifat bawah permukaan jari karena komponen darah (hemoglobin teroksigenasi dan terdeoksigenasi) menyerap panjang gelombang cahaya yang berbeda. Demikian pula, jaringan, darah, lemak, dan pigmen melanin di mata menyerap panjang gelombang cahaya yang berbeda.

Sifat-sifat ini dapat dimanfaatkan untuk deteksi keaktifan dalam sistem pengenalan sidik jari (lihat Gambar 7.8) dan iris. Mata memiliki beberapa sifat optik tambahan yang juga dapat digunakan untuk mendeteksi iris palsu. Misalnya, foto iris dapat dibedakan dari iris asli dengan mendeteksi fenomena seperti pantulan Purkinje dan efek mata merah. Sementara gambar Purkinje merupakan pantulan objek luar terhadap kornea mata, efek mata merah disebabkan oleh pantulan retina. Selain itu, analisis spektrum Fourier dua dimensi juga dapat digunakan untuk mengidentifikasi lensa kontak dengan iris palsu yang tercetak di atasnya (lihat Gambar 7.9)



Gambar 7.8 Contoh Deteksi Sidik Jari Palsu Menggunakan Sifat Spektral Jaringan Manusia.

a) *Sensor sidik jari multispektral dari Lumidigm, Inc. yang mampu menangkap sifat bawah permukaan jari.*
b) *Sidik jari palsu yang terbuat dari lem.*
c) *Cetakan jari asli yang diperoleh menggunakan sensor sidik jari optik tradisional (berdasarkan prinsip refleksi internal total (TIR)).*
d) *Cetakan jari asli yang diperoleh menggunakan sensor sidik jari multispektral.*
e) *Cetakan jari palsu (lem palsu yang dilapisi pada jari asli) yang diperoleh menggunakan sensor sidik jari optik, dan*
f) *Cetakan jari palsu yang diperoleh menggunakan sensor sidik jari multispektral. Dapat diamati bahwa sensor multispektral mampu melihat melalui palsu dan menangkap pola tonjolan jari asli yang mendasarinya.*



Gambar 7.9 Contoh deteksi spoof iris).

Iris yang dicetak biasanya menunjukkan beberapa artefak yang dapat dideteksi dengan menganalisis spektrum Fourier 2 dimensi dari gambar iris. Salah satu kritik umum terhadap algoritme deteksi keaktifan yang digunakan dalam sistem biometrik komersial adalah bahwa algoritme tersebut semata-mata didasarkan pada prinsip keamanan melalui ketidakjelasan. Dengan kata lain, vendor biometrik umumnya tidak mengungkapkan algoritme atau detail implementasi tentang metodologi deteksi keaktifan mereka karena jika spesifikasi teknik deteksi spoof terungkap, sistem dapat dielakkan dengan mudah. Pengalaman dalam sistem kriptografi telah menunjukkan bahwa pendekatan ini tidak memberikan hasil yang memuaskan dalam jangka waktu tertentu.

Karakteristik listrik

Konduktivitas listrik jaringan manusia berbeda dari konduktivitas banyak bahan sintetis lainnya seperti karet silikon dan gelatin. Konduktivitas bahan yang disajikan pada sensor sidik jari dapat diukur untuk membedakan jari asli dari jari palsu. Namun, konduktivitas jari asli sangat bervariasi tergantung pada kondisi lingkungan seperti kelembapan dan suhu. Jika air atau air liur ditambahkan ke jari palsu, konduktivitasnya mungkin tidak dapat dibedakan dari jari yang hidup.

Deformasi kulit

Pola deformasi kulit manusia dapat digunakan untuk membedakan jari yang hidup dari jari yang palsu. Kulit lebih fleksibel daripada kebanyakan bahan lain dan tonjolan serta lembah pada jari palsu tidak berubah bentuk seperti ujung jari yang hidup. Kulit asli hanya berubah bentuk dengan cara tertentu karena kulit tersebut melekat pada kulit di bawahnya dan deformasi dipengaruhi oleh posisi dan bentuk tulang jari. Namun, mengukur pola deformasi ini tidaklah mudah karena memerlukan perekaman video sidik jari pada frame rate yang tinggi saat jari bergerak pada permukaan sensor. Hal ini bermasalah karena sebagian besar sensor sidik jari dirancang untuk akuisisi sidik jari dengan satu sentuhan dan pengguna dilatih untuk tidak menggerakkan jari selama perekaman; deformasi yang berlebihan akan memengaruhi akurasi pencocokan sistem.

Setelah penyerang mengidentifikasi kemungkinan kerentanan dan berhasil melakukan serangan spoof, seluruh sistem akan hancur. Oleh karena itu, seseorang harus berasumsi bahwa penyerang memiliki pengetahuan tentang sifat fisiologis yang digunakan oleh sistem untuk mendeteksi spoof. Akibatnya, penyerang mungkin dapat membuat jari palsu dengan sifat yang sama yang diverifikasi oleh detektor spoof. Tentu saja, penambahan karakteristik fisiologis yang semakin banyak dalam proses deteksi spoof akan membuat penyerang semakin sulit (meskipun bukan tidak mungkin) untuk mengelabui sistem. Sementara sensor biometrik harus dilengkapi dengan kemampuan deteksi keaktifan sebanyak mungkin, penggunaan beberapa ciri biometrik (sistem biometrik multimoda dibahas dalam Bab 6) yang dikombinasikan dengan mekanisme tantangan-respons yang cerdas mungkin diperlukan untuk meningkatkan standar ke tingkat yang sulit diatasi oleh penyerang.

7.4 SERANGAN PADA PEMROSESAN BIOMETRIK

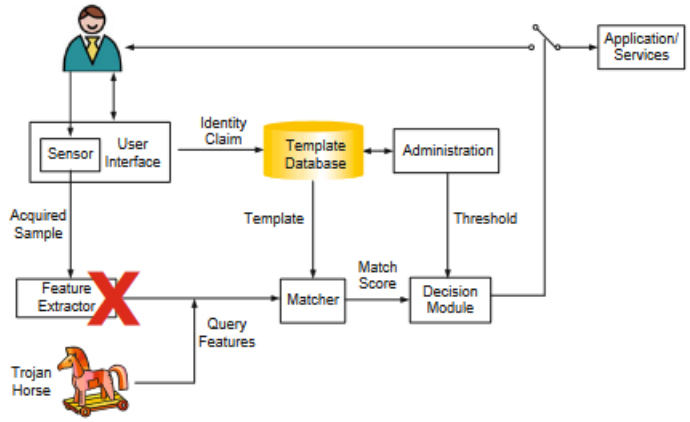
Algoritma pemrosesan sinyal dan pencocokan pola yang menjadi inti dari pengenalan biometrik otomatis diimplementasikan dalam modul sensor, ekstraktor fitur, pencocok, dan keputusan. Dengan demikian, penyerang dapat merusak pemrosesan biometrik baik dengan secara langsung merusak modul fungsional inti dari sistem biometrik atau dengan memanipulasi komunikasi antara modul-modul ini. Meskipun basis data templat juga merupakan salah satu modul dalam sistem biometrik, motivasi dan konsekuensi dari serangan pada basis data templat berbeda dibandingkan dengan modul lainnya. Oleh karena itu, serangan pada basis data templat akan dipertimbangkan secara terpisah.

Serangan Pada Modul Sistem

Serangan pada modul fungsional inti dapat dilakukan baik melalui modifikasi yang tidak sah atau dengan mengeksploitasi kesalahan dalam implementasinya. Motivasi dari serangan ini dapat menyebabkan penolakan layanan kepada pengguna yang sah atau memfasilitasi intrusi.

Modifikasi Yang Tidak Sah

Komponen perangkat keras dan perangkat lunak dari sistem biometrik dapat dimodifikasi oleh penyerang. Contoh klasiknya adalah modifikasi program yang dapat dieksekusi dalam suatu modul melalui serangan Trojan Horse. Trojan Horse adalah perangkat lunak berbahaya yang tampaknya menjalankan fungsi yang diinginkan oleh pengguna, tetapi sebaliknya menjalankan beberapa fungsi lain yang biasanya memudahkan intrusi oleh pengguna yang tidak sah. Trojan Horse dapat menyamar sebagai salah satu modul, melewati modul tersebut, dan mengeluarkan nilai yang diinginkan oleh penyerang sebagai input ke modul berikutnya. Misalnya, program Trojan Horse dapat melewati ekstraktor fitur dan mengirim fitur palsu yang ditentukan oleh penyerang ke modul pencocokan (lihat Gambar 7.10). Serangan serupa juga dapat dilakukan pada modul penginderaan, estimasi kualitas, pencocokan, basis data templat, dan keputusan.



Gambar 7.10 Serangan Trojan Horse Terhadap Modul Ekstraksi Fitur Ditunjukkan.

Trojan Horse adalah perangkat lunak berbahaya yang tampaknya menjalankan fungsi yang diinginkan oleh pengguna yang sah, tetapi sebaliknya menjalankan beberapa fungsi lain yang biasanya memfasilitasi intrusi oleh pengguna yang tidak sah. Dalam contoh ini, Trojan Horse menggantikan ekstraktor fitur dan mengeluarkan fitur yang diputuskan oleh penyerang, bukan fitur yang diekstrak dari ciri biometrik input. Jika sensor dan modul pencocok tidak menyadari fakta bahwa mereka berkomunikasi dengan Trojan Horse, dan bukan dengan ekstraktor fitur yang sebenarnya, hal itu akan menyebabkan penolakan layanan kepada pengguna asli atau intrusi oleh penyerang.

Salah satu metode untuk mengatasi serangan ini adalah dengan menggunakan sistem biometrik tepercaya. Sistem biometrik tepercaya adalah sistem di mana modul-modul yang berbeda terikat bersama secara fisik dan/atau logis menggunakan autentikasi bersama antara modul-modul tersebut. Autentikasi bersama menyiratkan bahwa kepercayaan dibangun di kedua arah antara dua pihak yang berkomunikasi. Hal ini biasanya dicapai

melalui protokol kriptografi kunci publik dan tanda tangan digital. Selain autentikasi bersama, praktik eksekusi kode aman atau perangkat keras khusus yang tahan terhadap gangguan yang dapat memaksakan eksekusi perangkat lunak yang aman dapat digunakan untuk menghindari modifikasi fungsionalitas modul.

Pemanfaatan Kesalahan

Penyerang dapat mengidentifikasi dan memanfaatkan celah dalam penerapan algoritme biometrik atau konfigurasi yang tidak aman untuk menghindari sistem biometrik. Sebagai contoh, pertimbangkan modul pencocokan di mana nilai input tertentu, misalnya $\mathbf{b_0}$, tidak ditangani dengan tepat, dan setiap kali $\mathbf{b_0}$ dimasukkan ke pencocok, ia selalu mengeluarkan keputusan "pencocokan". Kerentanan ini mungkin tidak memengaruhi fungsi normal sistem karena, dalam praktiknya, kemungkinan $\mathbf{b_0}$ dihasilkan dari data biometrik nyata mungkin dapat diabaikan. Namun, penyerang dapat memanfaatkan celah ini untuk dengan mudah melanggar keamanan tanpa terdeteksi.

Perlu dicatat bahwa penyerang mungkin perlu melewati satu atau beberapa modul dalam sistem biometrik untuk memanfaatkan kesalahan implementasi tersebut. Serangan ini juga terkait erat dengan serangan pengaburan, karena pengetahuan tentang kesalahan dalam implementasi biometrik akan memungkinkan penyerang untuk menghindari sistem melalui perubahan yang tepat pada sifat biometriknya. Serangan ini dapat dicegah dengan menggunakan algoritma biometrik yang telah teruji dengan baik.

Serangan Pada Interkoneksi

Tiga serangan berikut mungkin terjadi ketika penyerang memperoleh kendali atas antarmuka komunikasi antara berbagai modul sistem biometrik. Sementara serangan man-in-the-middle dan replay umum terjadi pada saluran komunikasi antara dua modul mana pun dalam sistem biometrik, serangan hill-climbing khusus terjadi pada tautan antara sensor dan ekstraktor fitur atau tautan antara ekstraktor fitur dan matcher.

Serangan Man-In-The-Middle

Dalam kriptografi, serangan man-in-the-middle merupakan bentuk penyadapan aktif, di mana penyerang membuat koneksi independen antara dua entitas yang sudah berkomunikasi dan menyampaikan pesan di antara keduanya. Korban diyakinkan bahwa mereka berkomunikasi secara langsung satu sama lain, padahal sebenarnya seluruh percakapan dikendalikan oleh penyerang. Dalam sistem biometrik, serangan man-in-the-middle dapat dilakukan terhadap dua modul biometrik mana pun dan efeknya sama dengan serangan Trojan horse pada modul sistem, yaitu memungkinkan penyerang untuk menyuntikkan nilai palsu ke dalam sistem biometrik. Autentikasi bersama antara modul biometrik diperlukan untuk melawan serangan ini.

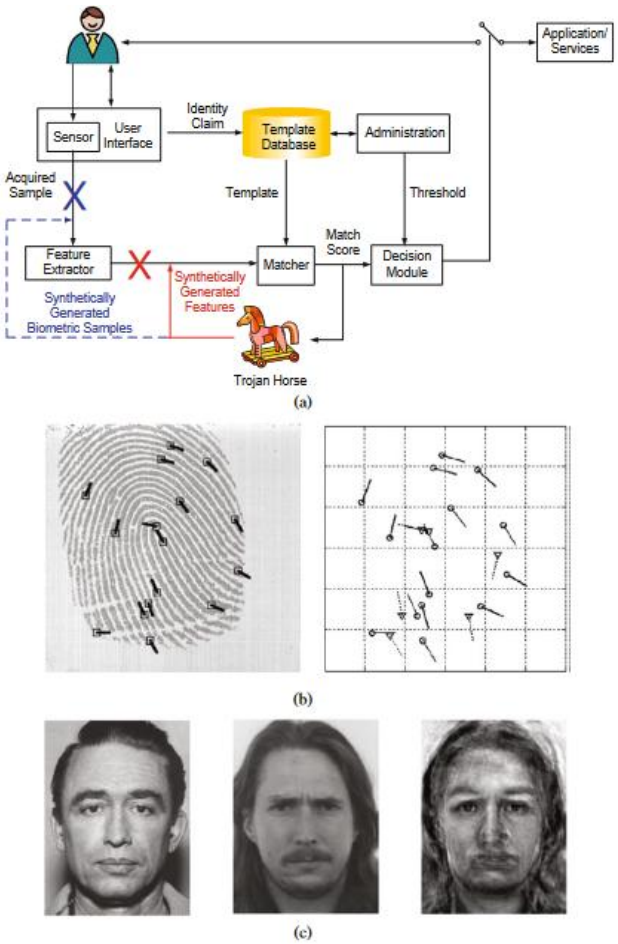
Serangan Replay

Jika saluran antara modul biometrik tidak diamankan secara fisik atau kriptografis, penyerang dapat menyadap data yang sedang ditransfer dan memutarnya kembali di lain waktu. Data biometrik mentah atau fitur yang diekstraksi dapat disadap dan diputar ulang. Serangan replay mungkin terjadi meskipun data dienkripsi. Tindakan balasan terhadap serangan ini adalah dengan menggunakan stempel waktu atau mekanisme

tantangan/respons. Autentikasi bersama antara modul dan penggunaan kunci sesi satu kali selama setiap transaksi juga dapat mengurangi serangan replay.

Serangan Hill-Climbing

Serangan Hill-climbing mungkin terjadi ketika (a) penyerang memiliki kemampuan untuk menyuntikkan data sampel biometrik mentah atau fitur secara langsung melalui serangan Trojan-horse atau serangan man-in-the-middle, dan (b) penyerang dapat memperoleh keluaran skor kecocokan oleh pencocok (lihat Gambar 7.11). Di sini, tujuan penyerang adalah untuk menentukan sampel biometrik atau set fitur yang cocok dengan identitas yang ditargetkan untuk algoritme biometrik yang ditentukan. Jelas, jika seseorang dapat menyuntikkan sampel biometrik atau vektor fitur yang sewenang-wenang dan memperoleh skor kecocokan dari sistem biometrik, seseorang dapat melancarkan serangan brute-force. Dalam kasus ini, penyerang dapat mencoba sampel yang berbeda dari basis data biometrik yang besar dan ia cenderung berhasil menemukan kecocokan yang dekat dalam sekitar (1/FMR) percobaan, di mana FMR adalah rasio kecocokan palsu dari sistem biometrik. Serangan brute-force semacam itu dalam sistem biometrik setara dengan serangan kamus dalam sistem autentikasi berbasis kata sandi.



Gambar 7.11 Proses Verifikasi Biometrik Dan Potensi Kerentanan Terhadap Serangan Sintetik

(a) Serangan hill climbing dapat dilakukan baik di ruang sampel biometrik maupun di ruang fitur. Di sini, tujuan penyerang adalah menentukan sampel biometrik atau set fitur yang cocok dengan identitas target. Misalkan Trojan horse menggantikan ekstraktor fitur dan menyuntikkan fitur yang dihasilkan secara sintetis. Umpan balik yang diperoleh melalui skor kecocokan dapat digunakan untuk memodifikasi fitur sintetis secara berulang hingga kecocokan ditemukan.

(b) Minutiae sidik jari yang diregenerasi. Sidik jari target dengan minutiae berlabel ditunjukkan di sebelah kiri dan posisi minutiae yang dipelajari menggunakan serangan hill-climbing ditunjukkan di sebelah kanan (garis solid dengan lingkaran $(-o)$ menunjukkan minutiae asli, garis putus-putus dengan segitiga $(-\nabla)$ menunjukkan minutiae sintetis.).

(c) Citra wajah yang diregenerasi. Dari kiri ke kanan: citra wajah target, citra awal yang dipilih untuk hill-climbing, dan citra wajah yang diregenerasi.

Keefisienan serangan brute-force mungkin dapat ditingkatkan jika informasi skor kecocokan tersedia. Hal ini mengarah pada serangan hill-climbing, di mana sampel biometrik atau set fitur yang dibuat secara artifisial pertama kali dimasukkan ke dalam sistem dan respons (skor kecocokan) dicatat. Penyerang kemudian mengganggu sampel atau set fitur awal, mengirimkannya ke sistem, dan mencatat skor kecocokan yang baru. Jika skor kecocokan pada iterasi kedua lebih tinggi dari yang pertama, perubahan dipertahankan; jika tidak, perubahan dibuang.

Proses di atas diulang beberapa kali hingga skor kecocokan melampaui ambang batas yang ditetapkan oleh administrator sistem. Pada setiap iterasi di mana skor kecocokan lebih tinggi dari sebelumnya, sampel atau set fitur yang dibuat secara artifisial menjadi lebih mirip dengan templat yang menjadi target. Seseorang dapat dengan mudah melihat bahwa serangan hill-climbing lebih sulit diimplementasikan daripada serangan Trojan horse atau man-in-the-middle. Alasan kesulitan ini adalah bahwa tidak hanya akses ke skor kecocokan yang dibutuhkan, penyerang juga perlu memiliki beberapa pengetahuan tentang distribusi fitur/sampel untuk secara sintetis menghasilkan fitur/sampel sedemikian rupa sehingga skor kecocokan yang lebih tinggi dapat diperoleh dalam iterasi berikutnya.

Namun, hasil bagi penyerang yang dihasilkan dari serangan hill-climbing secara signifikan lebih tinggi daripada serangan Trojan horse. Jika perkiraan yang baik dari sampel biometrik asli dari identitas target dapat diperoleh, itu mungkin dapat digunakan untuk membuat spoof atau untuk mengidentifikasi pengguna yang sama di berbagai aplikasi yang menggunakan sifat yang sama. Dengan demikian, serangan hill-climbing tidak hanya membahayakan integritas sistem biometrik yang diberikan, tetapi juga dapat membahayakan sistem biometrik lain yang menggunakan sifat yang sama. Membatasi jumlah percobaan kegagalan yang diizinkan dalam jangka waktu tertentu, meningkatkan ketelitian skor pencocokan, dan penggunaan sistem biometrik tepercaya adalah beberapa teknik yang dapat menangkal ancaman serangan pendakian bukit.

7.5 SERANGAN PADA BASIS DATA TEMPLAT

Ada dua jenis serangan yang mungkin terjadi pada basis data templat biometrik. Pertama, basis data templat dapat diretas atau dimodifikasi oleh penyerang untuk mendapatkan akses tidak sah atau untuk menolak akses bagi pengguna yang sah. Modifikasi

templat yang tidak sah ini dapat dilakukan tanpa memandang lokasi penyimpanan, baik itu server pusat, klien jarak jauh (misalnya, komputer pribadi, telepon seluler, dll.), atau kartu pintar. Serangan serupa juga mungkin terjadi dalam sistem autentikasi berbasis kata sandi. Teknik umum yang digunakan untuk mengurangi ancaman tersebut adalah dengan memiliki kontrol ketat pada akses basis data. Kedua, informasi templat biometrik yang tersimpan dapat tersedia bagi penyerang. Serangan semacam itu disebut kebocoran. Kebocoran bukanlah masalah serius dalam autentikasi berbasis kata sandi, karena hanya hash kriptografik dari kata sandi yang biasanya disimpan dalam basis data, dan penyerang tidak memperoleh informasi berguna dari mempelajari kata sandi yang di-hash ini. Namun, kebocoran merupakan masalah serius dalam sistem biometrik.

Ciri-ciri biometrik tidak selalu rahasia, dan kekuatan autentikasi biometrik terletak pada hubungan fisik yang kuat dan tidak dapat dibatalkan antara pengguna yang masih hidup dan ciri-ciri biometriknya, bukan pada kerahasiaan data biometrik. Oleh karena itu, wajar untuk bertanya-tanya mengapa kebocoran templat biometrik dari basis data merupakan masalah keamanan yang serius. Jawaban atas pertanyaan ini terletak pada pengamatan berikut.

Ada empat cara di mana informasi biometrik pengguna dapat diperoleh, yaitu, (a) kolusi atau paksaan, (b) akuisisi rahasia, (c) serangan brute-force atau hill-climbing, dan (d) kebocoran templat. Di antara keempat kemungkinan ini, dua kemungkinan pertama mengharuskan penyerang berada dalam jarak fisik yang dekat dengan pengguna atau mendapatkan kerja sama dari pengguna. Metode ketiga mengharuskan penyerang untuk melanggar keamanan sistem biometrik dan melancarkan serangan intrusi yang berhasil. Lebih jauh lagi, penyerang perlu mengeluarkan upaya yang signifikan dalam tiga metode pertama untuk memperoleh pengetahuan tentang satu pengguna. Sebaliknya, jika penyerang dapat meretas basis data biometrik yang besar, tugas yang dapat dilakukan dari lokasi yang jauh sambil tetap anonim, ia dapat dengan mudah memperoleh informasi biometrik tentang sejumlah besar pengguna beserta informasi biografi mereka (seperti nama, alamat, dll.).

Fakta bahwa pengenalan biometrik tidak bergantung pada kerahasiaan data biometrik hanya berlaku jika sistem dapat dengan andal membedakan antara penyajian pengguna yang masih hidup dan penyajian yang dipalsukan. Asumsi lainnya adalah bahwa infrastruktur biometrik tidak terganggu. Jika asumsi ini tidak terpenuhi, informasi biometrik yang bocor akan menyebabkan intrusi karena penyerang dapat merekayasa ulang templat untuk membuat spoof fisik atau memutar ulang templat yang dicuri untuk mendapatkan akses yang tidak sah.

Terakhir, kebocoran templat biometrik melanggar persyaratan kerahasiaan data dari sistem biometrik. Lebih jauh, tidak seperti kata sandi dan token, tidak mungkin mengganti ciri biometrik yang dikompromikan. Setelah informasi biometrik jatuh ke tangan musuh, informasi tersebut akan hilang selamanya dan tidak dapat diterbitkan kembali, diperbarui, atau dihancurkan. Dengan demikian, sifat ciri biometrik yang tidak dapat dibatalkan, yang merupakan salah satu kekuatan pengenalan biometrik, juga dapat dianggap sebagai

kelemahan. Untuk lebih memperparah masalah ini, templat biometrik yang bocor dapat digunakan untuk tujuan sekunder seperti pencocokan silang di berbagai basis data untuk melacak seseorang secara diam-diam tanpa persetujuannya, sehingga mengakibatkan perambahan fungsi.

Dengan demikian, serangan kebocoran tidak hanya merupakan ancaman keamanan yang serius, tetapi juga merusak privasi pengguna. Karena alasan-alasan ini, perlindungan templat biometrik merupakan masalah yang sangat penting untuk ditangani, terutama dalam aplikasi yang memerlukan penyimpanan data biometrik di server pusat.

Penanggulangan: Keamanan Templat Biometrik

Karena masalah keamanan templat biometrik cukup mirip dengan masalah penyimpanan kata sandi secara aman, wajar dan intuitif untuk mempertimbangkan penggunaan kembali teknik yang sama yang dikembangkan untuk keamanan kata sandi guna melindungi templat biometrik. Tinjauan singkat tentang metodologi yang digunakan dalam keamanan kata sandi disajikan (lihat Gambar 7.12) sebelum membahas algoritme perlindungan templat biometrik.

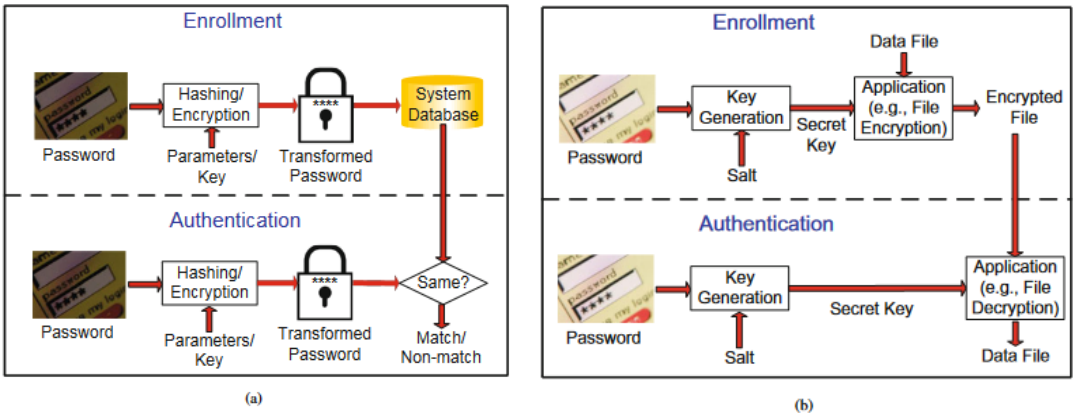
Teknik Untuk Mengamankan Kata Sandi

Salah satu pendekatan yang mungkin untuk mengamankan kata sandi adalah dengan mengenkripsinya menggunakan teknik kriptografi yang terkenal (misalnya, Advanced Encryption Standard (AES), algoritme Rivest-Shamir-Adleman (RSA), dll.) dan hanya menyimpan kata sandi yang dienkripsi. Selama autentikasi, algoritme enkripsi yang sama dapat diterapkan pada kata sandi input dan langsung dicocokkan dengan kata sandi terenkripsi yang tersimpan. Karena kata sandi terenkripsi dapat didekripsi jika kunci dekripsi diketahui, keamanan enkripsi bergantung pada kerahasiaan kunci dekripsi. Sudah diketahui umum bahwa manajemen kunci (pembuatan, pendistribusian, dan penyimpanan kunci kriptografi yang aman) mungkin merupakan masalah yang paling menantang dalam penerapan praktis kriptosistem. Bahkan jika kunci dekripsi disimpan dengan aman, penyerang dapat memilih beberapa kata sandi acak dan memperoleh kata sandi terenkripsi yang sesuai. Hal ini memungkinkan penyerang untuk mendapatkan kembali kunci rahasia melalui apa yang dikenal sebagai serangan teks biasa yang dipilih1. Karena keterbatasan ini, enkripsi kata sandi sederhana tidak cukup untuk mengamankan kata sandi. Alternatif kedua disebut sebagai pembuatan kunci berbasis kata sandi (lihat Gambar 7.12(b)). Dalam kasus ini, kata sandi tidak pernah disimpan di mana pun dalam sistem.

Sebaliknya, kata sandi tersebut langsung digunakan untuk memperoleh kunci kriptografi yang biasanya dikombinasikan dengan informasi acak tambahan yang dikenal sebagai salt. Aplikasi lain seperti sistem enkripsi berkas dapat langsung menggunakan kunci yang diperoleh dari kata sandi untuk kriptografi kunci simetris. Meskipun pendekatan ini bermanfaat dalam arti bahwa kata sandi tidak perlu disimpan di mana pun, pendekatan ini hanya dapat digunakan dalam aplikasi yang autentikasinya tersirat. Misalnya, seseorang dapat mendekripsi berkas terenkripsi dan membaca isinya hanya jika kata sandi yang tepat diberikan.

Pendekatan ketiga yang digunakan dalam sebagian besar sistem autentikasi berbasis kata sandi modern adalah menerapkan fungsi hash kriptografi pada kata sandi teks biasa dan hanya menyimpan kata sandi yang di-hash. Ketika pengguna memasukkan kata sandi selama autentikasi, fungsi hash yang sama diterapkan pada kata sandi input dan nilai hash yang dihasilkan secara langsung dicocokkan dengan nilai hash yang disimpan (lihat Gambar 7.12(a)). Fungsi hash kriptografi yang baik h(.) setidaknya harus memenuhi tiga properti berikut :

1. Resistensi pra-citra: Jika diberikan kata sandi yang di-hash secara kriptografi, misalnya h(x), maka secara komputasi pasti sulit untuk menemukan kata sandi y sehingga h(y)= h(x).
2. Resistensi benturan yang lemah: Jika diberikan x dan h(x), maka secara komputasi pasti sulit untuk menemukan y, di mana y = x, sehingga h(y)= h(x), dan
3. Resistensi benturan: Pasti sulit secara komputasi untuk menemukan beberapa x dan y yang sembarangan, sehingga x ≠ y, tetapi h(x)= h(y). Dengan kata lain, sulit untuk menemukan dua kata sandi yang berbeda yang menghasilkan hash kriptografi yang sama. Perhatikan bahwa resistensi benturan yang lemah tidak menyiratkan resistensi benturan. Karena sifat-sifat fungsi hash di atas, bahkan jika kata sandi yang disimpan (di-hash) menjadi tersedia bagi penyerang, hal itu tidak mengakibatkan ancaman keamanan yang serius.



Gambar. 7.12 Pendekatan Yang Digunakan Untuk Mengamankan Kata Sandi.

(a) Dalam enkripsi atau hashing kata sandi, hanya kata sandi terenkripsi atau hash kriptografik dari kata sandi yang disimpan dalam basis data. Sementara pendekatan enkripsi mengharuskan kunci dekripsi disimpan dengan aman, sifat non-invertibilitas dari fungsi hash kriptografik melindungi kata sandi bahkan jika fungsi hash dan parameternya tersedia bagi penyerang. Oleh karena itu, hashing umumnya lebih disukai daripada enkripsi dalam konteks keamanan kata sandi.

(b) Dalam pembuatan kunci berbasis kata sandi, kata sandi tidak pernah disimpan di mana pun dalam sistem. Sebaliknya, kata sandi digunakan untuk memperoleh kunci kriptografik yang biasanya dikombinasikan dengan informasi acak tambahan yang dikenal sebagai salt. Kunci yang dihasilkan dari kata sandi ini dapat langsung digunakan dalam aplikasi lain seperti sistem enkripsi file.

Tantangan Dan Persyaratan Dalam Keamanan Templat Biometrik

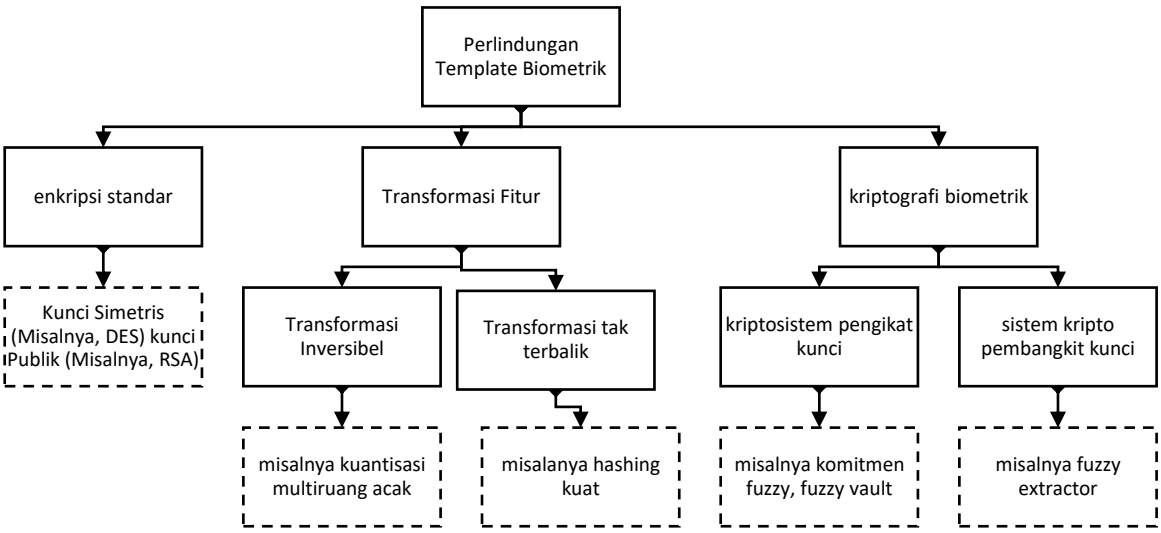
Apakah mungkin untuk langsung menerapkan salah satu dari tiga pendekatan keamanan kata sandi di atas untuk menghasilkan templat biometrik yang "aman"? Sayangnya, jawaban untuk pertanyaan di atas adalah negatif dan alasannya terletak pada perbedaan mendasar antara sistem autentikasi berbasis kata sandi dan biometrik yang disorot dalam Bab 1. Sementara autentikasi berbasis kata sandi bergantung pada kecocokan persis antara kata sandi yang dimasukkan selama pendaftaran dan autentikasi, pengenalan biometrik didasarkan pada kecocokan tidak persis antara sampel pendaftaran dan autentikasi. Faktanya, seperti yang ditunjukkan sebelumnya, dapat terjadi variabilitas intra-pengguna yang besar dalam beberapa akuisisi sifat biometrik yang sama dan penanganan variasi intra-pengguna ini merupakan tantangan terpenting dalam merancang skema perlindungan templat biometrik. Oleh karena itu, istilah templat "terlindungi" atau "aman" akan digunakan untuk merujuk pada templat yang diperoleh setelah penerapan algoritma keamanan templat biometrik ke templat "tidak terlindungi" atau "asli".

Skema perlindungan templat biometrik harus memiliki tiga properti berikut:

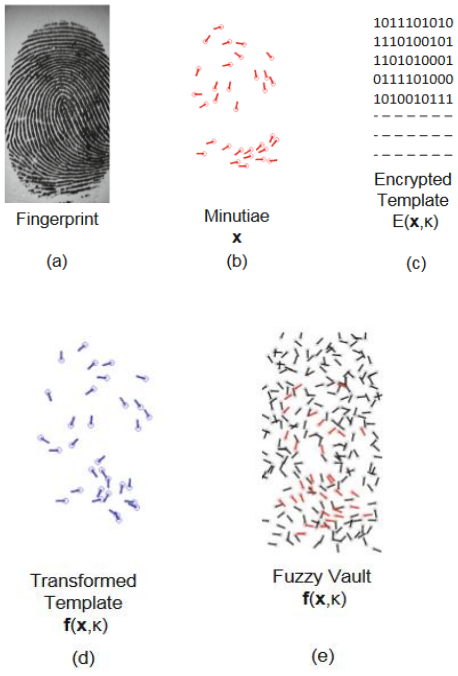
1. Keamanan kriptografi: Keamanan kriptografi mengacu pada properti ketahanan pracitra yang biasanya dipenuhi oleh fungsi hash kriptografi. Dengan adanya templat yang aman, pasti sulit secara komputasi untuk menemukan set fitur biometrik (umumnya dikenal sebagai pracitra) yang akan cocok dengan templat yang aman. Properti ini melindungi dari kemungkinan penyerang menyusup ke dalam sistem biometrik yang sedang dipertimbangkan dengan memutar ulang pracitra. Konsep ketahanan pracitra juga terkait dengan fungsi matematika satu arah atau tidak dapat dibalik. Fungsi f disebut sebagai fungsi satu arah jika "mudah dihitung" (dalam waktu polinomial) tetapi "sulit dibalik" (dengan f(x), probabilitas menemukan x dalam waktu polinomial kecil). Skema perlindungan templat yang tidak dapat dibalik menyiratkan bahwa akan sulit secara komputasi untuk memperoleh fitur biometrik asli dari templat yang aman. Hal ini mencegah penyerang membuat tiruan fisik dari ciri biometrik dan menyusup ke sistem biometrik lain yang menggunakan ciri biometrik yang sama. Dengan demikian, templat yang aman harus tahan terhadap pra-citra dan tidak dapat dibalik.
2. Kinerja: Skema perlindungan templat biometrik tidak boleh menurunkan kinerja pengenalan (FMR dan FNMR) sistem biometrik.
3. Dapat dibatalkan: Sebaiknya ada skema perlindungan templat yang dapat menghasilkan beberapa templat aman dari data biometrik yang sama. Beberapa templat aman ini harus sedemikian rupa sehingga meskipun penyerang memperoleh dua atau lebih templat, secara komputasi akan sulit untuk (a) mengidentifikasi bahwa templat tersebut berasal dari data biometrik yang sama dan (b) memperoleh ciri biometrik asli pengguna.

Properti yang dapat dibatalkan atau dapat dibatalkan ini memastikan bahwa pencocokan silang di seluruh basis data biometrik tidak memungkinkan, sehingga menjaga privasi pengguna. Dapat dibatalkan juga memudahkan untuk membuang templat yang disusupi

dan menerbitkan kembali templat baru berdasarkan data biometrik yang sama. Idealnya, skema perlindungan templat harus memenuhi ketiga persyaratan tersebut secara bersamaan. Akan tetapi, merancang teknik semacam itu merupakan tantangan tersendiri. Bagian berikut mempertimbangkan berbagai cara untuk mengamankan templat biometrik dan menganalisis bagaimana skema ini dibandingkan satu sama lain berdasarkan ketiga persyaratan di atas. Gambar 7.13 menyajikan kategorisasi umum algoritma perlindungan templat biometrik dan Gambar 7.14 menunjukkan ilustrasi pendekatan perlindungan templat utama saat diterapkan pada templat detail sidik jari.



Gambar. 7.13 Berbagai pendekatan untuk mengamankan templat biometrik.

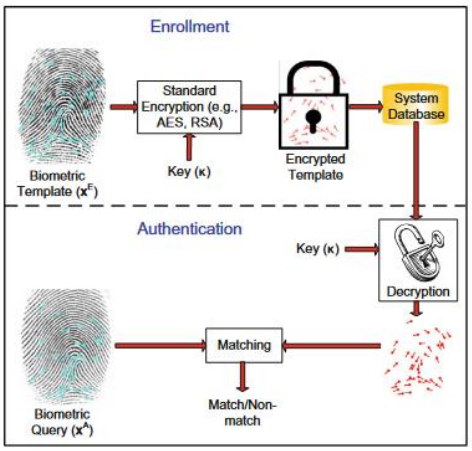


Gambar 7.14 Ilustrasi Pendekatan Perlindungan Templat Yang Berbeda Saat Diterapkan Pada Templat Minutiae Sidik Jari

(a) Sampel sidik jari yang diperoleh selama pendaftaran,
(b) Templat minutiae yang diekstraksi dari sampel pendaftaran,
(c) Templat sidik jari yang dienkripsi menggunakan algoritma enkripsi standar seperti AES,
(d) Templat minutiae yang ditransformasikan yang diperoleh menggunakan skema transformasi yang tidak dapat dibalikkan, dan
(e) Brankas fuzzy (sistem kriptografi biometrik) yang menyembunyikan templat minutiae di antara sekumpulan besar titik sekam acak.

Pendekatan Enkripsi Standar

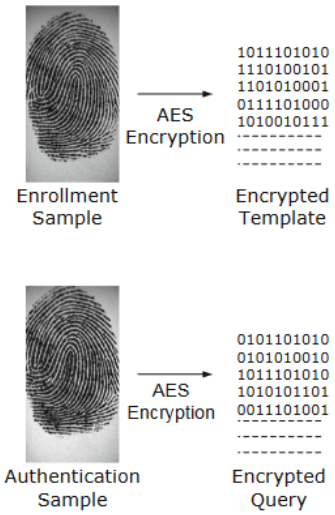
Cara paling sederhana untuk mengamankan templat biometrik adalah dengan mengenkripsinya menggunakan teknik kriptografi standar seperti RSA dan AES. Ini adalah metodologi yang digunakan di sebagian besar sistem biometrik komersial yang ada. Namun, seperti yang ditunjukkan pada Gambar 7.15, solusi enkripsi dalam kasus templat biometrik tidak setara dengan skenario enkripsi kata sandi karena alasan berikut.



Gambar. 7.15 Mengamankan Templat Biometrik Melalui Teknik Enkripsi Standar.

Tidak seperti enkripsi kata sandi, pencocokan biometrik tidak dapat dilakukan dalam domain terenkripsi karena adanya variasi intra-pengguna dalam data biometrik. Karena enkripsi sederhana dan tidak memengaruhi kinerja pengenalan, enkripsi digunakan secara luas dalam banyak sistem biometrik yang ada. Namun, templat tersebut aman hanya jika kunci kriptografi (κ) dirahasiakan dan pencocokan dilakukan dalam lingkungan tepercaya.

Ingatlah bahwa beberapa akuisisi dari ciri biometrik yang sama tidak menghasilkan set fitur yang sama. Biasanya, fungsi enkripsi standar bukanlah fungsi yang lancar dan sedikit perbedaan dalam nilai set fitur yang diekstraksi dari data biometrik mentah akan menyebabkan perbedaan yang sangat besar dalam fitur terenkripsi yang dihasilkan (lihat Gambar 7.16).



Gambar 7.16 Ilustrasi Perbedaan Besar Dalam Templat Terenkripsi Dan Kueri Terenkripsi Saat Fitur Yang Diekstrak Dari Beberapa Tayangan Sidik Jari Yang Sama Dienkripsi Menggunakan Teknik Enkripsi Standar (Misalnya, AES, RSA).

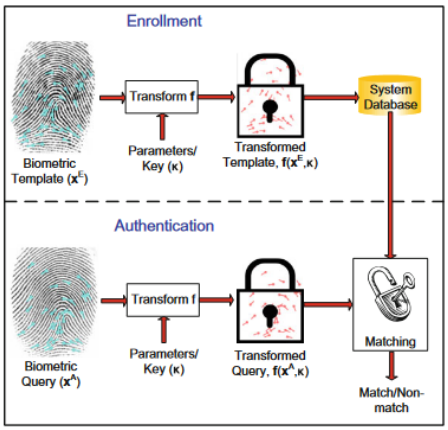
Akibatnya, tidak seperti enkripsi kata sandi, seseorang tidak dapat melakukan pencocokan secara langsung di domain terenkripsi. Sebaliknya, templat harus didekripsi agar dapat dicocokkan dengan fitur kueri. Akibatnya, fitur biometrik asli terekspos selama setiap upaya autentikasi, terlepas dari apakah autentikasi akhirnya berhasil. Keuntungan utama dari pendekatan enkripsi standar adalah bahwa kinerja pengenalan sistem biometrik tidak terpengaruh sama sekali. Karena pencocokan benar-benar terjadi di domain yang didekripsi, tidak perlu mendesain ulang atau memodifikasi algoritma pencocokan yang tersedia. Inilah alasan popularitas pendekatan ini. Namun, harus ditekankan bahwa solusi enkripsi aman dan dapat dibatalkan hanya dalam kondisi ideal (kunci dirahasiakan dan pencocokan dilakukan di lokasi tepercaya). Jika masalah praktis seperti manajemen kunci atau kerentanan terhadap pencurian templat selama upaya pencocokan diperhitungkan, teknik enkripsi standar tidak cukup baik untuk mengamankan templat biometrik.

Untuk mengatasi masalah ini, sejumlah teknik telah diusulkan, yang secara khusus dirancang untuk keamanan templat biometrik, dengan mempertimbangkan karakteristik unik domain ini seperti variasi intra-pengguna. Teknik-teknik ini secara kasar dapat diklasifikasikan sebagai pendekatan transformasi fitur dan kriptosistem biometrik. Namun, kedua pendekatan ini tidak saling eksklusif dan banyak algoritma perlindungan templat yang diusulkan dalam literatur memanfaatkan ide-ide dari kedua metodologi ini. Ketika skema keamanan templat secara jelas melibatkan elemen dari kedua pendekatan dasar, skema tersebut disebut sebagai kriptosistem biometrik hibrid.

Pendekatan Transformasi Fitur

Dalam pendekatan transformasi fitur, fungsi transformasi $f(.)$ diterapkan pada templat biometrik X^Edan hanya templat yang ditransformasikan f(X^E , κ) yang disimpan dalam basis data. Parameter fungsi transformasi biasanya berasal dari kunci acak, κ, atau kata sandi. Fungsi transformasi yang sama diterapkan pada fitur kueri, X^A, dan kueri yang

ditransformasikan, f(X^E, κ), secara langsung dicocokkan dengan templat yang ditransformasikan, f(X^E, κ). Dari Gambar 7.17, kita dapat melihat dengan jelas bahwa pendekatan transformasi fitur serupa dengan enkripsi atau hashing kata sandi. Bergantung pada karakteristik fungsi transformasi f, skema transformasi fitur dapat dikategorikan lebih lanjut sebagai transformasi yang dapat dibalik dan yang tidak dapat dibalik.



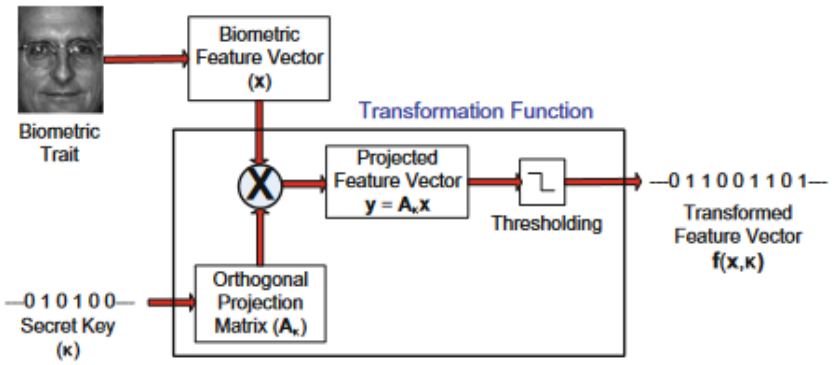
Gambar 7.17 Mengamankan Templat Biometrik Menggunakan Pendekatan Transformasi Fitur.

Transformasi yang dapat dibalik: Saat fungsi transformasi, f(.), dapat dibalik, keamanan templat yang ditransformasi didasarkan pada kerahasiaan kunci κ. Dengan kata lain, jika penyerang memperoleh akses ke kunci dan templat yang ditransformasi, ia dapat memulihkan templat biometrik asli (atau perkiraan yang mendekati). Dengan demikian, templat yang dilindungi menggunakan pendekatan transformasi fitur yang dapat dibalik mirip dengan kata sandi terenkripsi. Seperti dalam kasus enkripsi kata sandi, kesulitan praktis dalam manajemen kunci membatasi keamanan pendekatan transformasi yang dapat dibalik.

Selain itu, algoritma pencocokan perlu didesain ulang untuk memungkinkan pencocokan dalam domain yang ditransformasi. Namun, jika kunci dibuat khusus untuk pengguna dan jika kunci khusus pengguna ini diasumsikan sebagai rahasia yang hanya diketahui oleh pengguna yang sah, ada dua keuntungan potensial. Pertama, penggunaan informasi acak tambahan dalam bentuk kunci khusus pengguna biasanya meningkatkan keterpisahan antara pengguna dalam ruang fitur. Akibatnya, kemampuan diskriminasi dalam domain yang ditransformasikan lebih tinggi daripada dalam domain fitur asli, yang mengarah ke tingkat kecocokan palsu yang lebih rendah. Kedua, kunci khusus pengguna memfasilitasi pembatalan templat yang ditransformasikan.

Contoh terkenal dari pendekatan transformasi fitur yang dapat dibalik adalah teknik kuantisasi multiruang acak (lihat Gambar 7.18). Skema ini dapat digunakan untuk mengubah vektor fitur biometrik dengan panjang tetap (dan biasanya bernilai riil). Pertimbangkan vektor fitur x ∈ $\mathbb{R}^d$. Kunci rahasia κ digunakan sebagai benih untuk secara acak menghasilkan matriks proyeksi ortogonal m × d A_κ , yang peringkatnya biasanya kurang dari d. Vektor fitur

x diproyeksikan ke subruang ortogonal acak (A_κ x) dan peta individual dikuantisasi (biasanya menjadi nilai biner) untuk mengompensasi variasi intra-pengguna. Ambang batas untuk binerisasi dipilih berdasarkan kriteria bahwa jumlah nol yang diharapkan dalam templat sama dengan jumlah satu yang diharapkan sehingga dapat memaksimalkan entropi templat.



Gambar 7.18 Mengamankan Templat Biometrik Menggunakan Teknik Kuantisasi Multiruang Acak.

Keamanan kriptografi templat bergantung pada karakteristik fungsi transformasi, f(.). Jika transformasi dapat dibalik, templat aman hanya jika kunci κ dijaga secara rahasia. Di sisi lain, templat yang diperoleh melalui transformasi yang tidak dapat dibalik biasanya aman, bahkan jika parameter transformasi diketahui.

Keamanan dalam skema ini disediakan oleh matriks proyeksi acak khusus pengguna A_κ. Jika penyerang memperoleh akses ke matriks ini, maka skema tersebut tidak tahan terhadap pra-citra atau tidak dapat dibalik. Meskipun matriks A_κ tidak memiliki kebalikan yang tepat karena peringkatnya kurang dari d, seseorang dapat dengan mudah memperoleh pra-citra dengan menghitung kebalikan semu dari A_κ. Lebih jauh, mungkin juga untuk memulihkan perkiraan dekat dari fitur biometrik asli (beberapa informasi hilang karena binerisasi) melalui serangan hill-climbing. Akhirnya, serangan yang mirip dengan serangan plaintext yang dipilih dapat digunakan untuk memulihkan matriks proyeksi acak secara langsung.

Teknik potensial lain yang dapat digunakan sebagai transformasi fitur yang dapat dibalik adalah enkripsi homomorfik. Kriptosistem homomorfik adalah sistem kriptografi yang memungkinkan operasi aljabar tertentu dilakukan pada teks biasa dengan melakukan operasi matematika (yang mungkin berbeda) pada teks sandi dan mendekripsi nilai yang diperoleh. Misalnya, algoritma RSA bersifat homomorfik terhadap perkalian, yaitu, jika hasil perkalian dua teks sandi yang dihasilkan menggunakan kunci yang sama didekripsi, hasilnya sama dengan hasil perkalian teks biasa yang sesuai. Properti homomorfik dari skema enkripsi dapat dimanfaatkan untuk secara langsung melakukan pencocokan biometrik dalam domain terenkripsi, seperti dalam kasus enkripsi kata sandi.

Transformasi yang tidak dapat dibalik

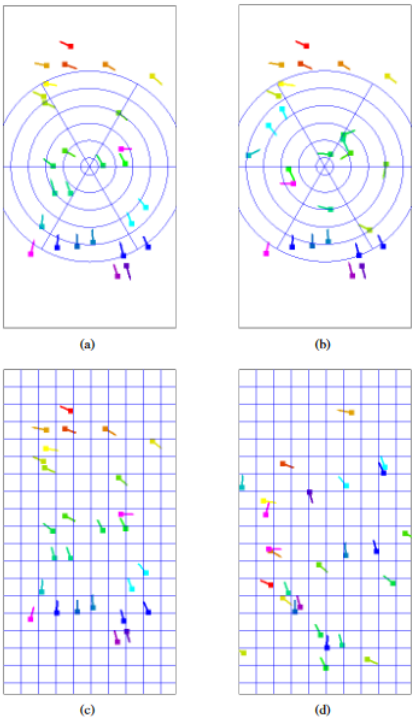
Skema transformasi yang tidak dapat dibalik biasanya menerapkan fungsi satu arah pada templat, dan secara komputasi sulit untuk membalikkan templat yang ditransformasikan bahkan jika kuncinya diketahui. Idealnya, seseorang harus menggunakan fungsi transformasi yang tahan terhadap pra-gambar dan tidak dapat dibalik. Jika transformasi tersebut dapat diterapkan, maka transformasi yang tidak dapat dibalik setara dengan skema hash kata sandi. Karena sulit untuk memulihkan templat biometrik asli bahkan ketika parameter transformasi dikompromikan, skema ini memberikan keamanan yang lebih baik daripada pendekatan transformasi yang dapat dibalik. Dengan memilih parameter transformasi khusus pengguna, pendekatan ini juga dapat memungkinkan pembatalan.

Kelemahan utama dari pendekatan ini adalah trade-off antara kemampuan membedakan (kinerja pengenalan) dan kemampuan tidak dapat dibalik (keamanan) dari fungsi transformasi. Fungsi transformasi harus mempertahankan kemampuan membedakan (struktur kesamaan) dari set fitur, yaitu, seperti di ruang fitur asli, fitur dari pengguna yang sama harus memiliki kesamaan yang tinggi di ruang yang ditransformasikan dan fitur dari pengguna yang berbeda harus sangat berbeda setelah transformasi. Di sisi lain, transformasi juga harus tidak dapat dibalik, yaitu, mengingat set fitur yang ditransformasikan, akan sulit bagi musuh untuk mendapatkan set fitur asli (atau perkiraan yang mendekatinya). Sulit untuk merancang fungsi transformasi yang memenuhi kondisi diskriminasi dan non-invertibilitas secara bersamaan. Selain itu, seseorang perlu memilih fungsi transformasi yang tepat berdasarkan karakteristik fitur biometrik yang digunakan dalam aplikasi tertentu.

Variasi intra-pengguna biasanya ditangani dengan menggunakan fungsi transformasi yang toleran terhadap variasi input. Alternatifnya adalah menggunakan fungsi transformasi yang tidak dapat dibalik yang meninggalkan templat biometrik di ruang (fitur) asli bahkan setelah transformasi (misalnya, detail sidik jari dapat diubah menjadi set detail lain dengan cara yang tidak dapat dibalik). Dalam skenario terakhir ini, variasi intra-pengguna dapat ditangani dengan menerapkan pencocok biometrik yang sama pada fitur yang diubah seperti pada set fitur asli. Templat yang berada di ruang yang sama setelah penerapan transformasi yang tidak dapat dibalik disebut sebagai templat yang dapat dibatalkan.

Contoh fungsi yang tidak dapat dibalik yang telah diusulkan untuk tujuan mengubah detail sidik jari meliputi transformasi kartesian, polar, dan fungsional. Dalam transformasi kartesian, ruang minutiae (citra sidik jari) ditesel menjadi kisi persegi panjang dan setiap sel (mungkin berisi beberapa minutiae) digeser ke posisi baru dalam kisi yang sesuai dengan translasi yang ditetapkan oleh kunci κ. Transformasi polar mirip dengan transformasi kartesian dengan perbedaan bahwa citra sekarang ditesel menjadi sejumlah cangkang konsentris dan setiap cangkang dibagi menjadi beberapa sektor. Karena ukuran sektor dapat berbeda (sektor yang dekat dengan pusat lebih kecil daripada yang jauh dari pusat), pembatasan biasanya ditempatkan pada vektor translasi yang dihasilkan dari kunci sehingga jarak radial sektor yang ditransformasikan tidak jauh berbeda dari jarak radial posisi asli.

Ilustrasi minutiae sebelum dan sesudah transformasi polar dan kartesian ditunjukkan pada Gambar 7.19.



Gambar 7.19 Ilustrasi Fungsi Transformasi Kartesian Dan Polar Untuk Menghasilkan Templat Sidik Jari Yang Dapat Dibatalkan.

(a) Minutiae asli pada kisi radial,
(b) Minutiae yang ditransformasikan setelah transformasi polar,
(c) Minutiae asli pada kisi persegi panjang, dan,
(d) Minutiae yang ditransformasikan setelah transformasi kartesian. Perhatikan bahwa minutiae diarsir secara berbeda untuk melacaknya setelah transformasi.

Untuk transformasi fungsional, campuran Gaussian 2D atau medan potensial listrik dalam distribusi muatan acak 2D dapat digunakan untuk menentukan translasi titik-titik minutiae. Besarnya fungsi-fungsi ini pada titik yang sesuai dengan minutia dapat digunakan sebagai ukuran besarnya translasi dan gradien suatu fungsi dapat digunakan untuk memperkirakan arah translasi minutia. Dalam ketiga transformasi tersebut, dua atau lebih minutia mungkin dapat dipetakan ke titik yang sama dalam domain yang ditransformasikan. Misalnya, dalam transformasi cartesian, dua atau lebih sel dapat dipetakan ke satu sel sehingga bahkan jika seorang penyerang mengetahui kunci dan karenanya, transformasi antara sel-sel, ia tidak dapat menentukan sel asli tempat minutia berada karena masing-masing minutia dapat secara independen menjadi milik salah satu sel yang mungkin. Ini memberikan jumlah non-invertibilitas yang terbatas pada transformasi. Juga, karena transformasi yang digunakan halus secara lokal, tingkat kesalahan tidak terpengaruh secara signifikan dan kemampuan membedakan minutia dipertahankan hingga tingkat yang besar. Dalam kasus transformasi minutiae sidik jari, kunci untuk mencapai kinerja pengenalan yang baik adalah ketersediaan

algoritma penyelarasan yang dapat secara akurat melakukan pra-penyelarasan (pendaftaran) gambar sidik jari atau fitur minutiae sebelum transformasi (misalnya, berdasarkan inti dan delta di sidik jari).

Kriptosistem Biometrik

Kriptosistem biometrik agak mirip dengan sistem pembuatan kunci berbasis kata sandi karena awalnya dikembangkan untuk tujuan mengamankan kunci kriptografi menggunakan fitur biometrik atau secara langsung membuat kunci kriptografi dari fitur biometrik. Karena fitur biometrik yang tersedia selama pendaftaran dan autentikasi berbeda, fitur-fitur ini tidak dapat langsung digunakan untuk pembuatan kunci kriptografi. Untuk memfasilitasi pembuatan kunci, beberapa informasi publik tentang fitur biometrik disimpan dalam basis data selama pendaftaran. Informasi publik ini biasanya disebut sebagai data pembantu atau sketsa aman dan karenanya, kriptosistem biometrik juga dikenal sebagai metode berbasis data pembantu. Sketsa aman digunakan selama autentikasi untuk mengekstrak kunci kriptografi dari fitur biometrik kueri melalui proses yang dikenal sebagai mekanisme pemulihan. Pencocokan dilakukan secara tidak langsung dengan memverifikasi validitas kunci yang diekstraksi atau dengan langsung menggunakan kunci tersebut di aplikasi lain.

Kriptosistem biometrik dapat diklasifikasikan lebih lanjut sebagai sistem pengikatan kunci dan pembuatan kunci tergantung pada bagaimana sketsa aman diperoleh. Ketika sketsa aman diperoleh dengan mengikat kunci kriptografi (yang independen dari fitur biometrik) dengan templat biometrik, maka sketsa tersebut disebut sebagai kriptosistem biometrik pengikat kunci. Jika data pembantu hanya berasal dari templat biometrik dan kunci kriptografi secara langsung dihasilkan dari data pembantu dan fitur biometrik kueri, maka sketsa tersebut mengarah ke kriptosistem biometrik pembangkit kunci.

Penting untuk ditekankan bahwa sketsa aman tidak harus dirahasiakan. Oleh karena itu, sketsa tersebut tidak boleh mengungkapkan informasi penting apa pun tentang templat biometrik asli (maka templat tersebut aman) atau kunci kriptografi (maka kuncinya aman). Dengan demikian, kriptosistem biometrik memecahkan masalah yang menantang dari manajemen kunci kriptografi dan perlindungan templat biometrik secara bersamaan. Karena alasan ini, topik ini sedang diteliti secara aktif baik dalam komunitas biometrik maupun kriptografi.

Mekanisme pemulihan dalam kriptosistem biometrik mampu mengompensasi variasi intra-pengguna dalam data biometrik, biasanya melalui penggunaan teknik pengkodean koreksi kesalahan. Pengodean koreksi kesalahan umumnya digunakan dalam sistem telekomunikasi untuk memungkinkan pengiriman data digital yang andal melalui saluran komunikasi yang tidak andal. Skema ini mencapai toleransi terhadap kesalahan dengan menambahkan informasi tambahan (redundan) ke pesan sebelum transmisi. Dalam konteks kriptosistem biometrik, fitur biometrik yang tersedia selama pendaftaran dianalogikan dengan pesan yang dikirimkan dalam sistem telekomunikasi. Data pembantu atau sketsa aman kira-kira setara dengan informasi redundan yang ditambahkan ke pesan. Fitur biometrik kueri bersama dengan sketsa aman membentuk pesan yang diterima. Asalkan

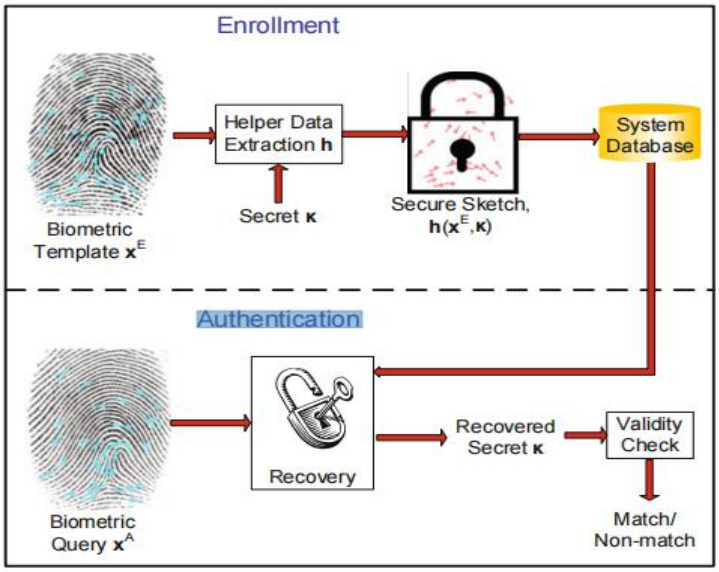
kueri cukup "dekat" dengan templat biometrik yang didaftarkan, templat biometrik asli dapat dipulihkan setelah koreksi kesalahan.

Tentu saja, kemampuan kriptosistem biometrik untuk menangani variasi intra-pengguna secara langsung bergantung pada jumlah informasi redundan (data pembantu) yang digunakan untuk koreksi kesalahan. Redundansi yang lebih tinggi umumnya mengarah pada toleransi kesalahan yang lebih tinggi dan akibatnya, stabilitas kunci yang lebih besar. Di sini, stabilitas kunci mengacu pada kemungkinan memulihkan kunci rahasia yang benar atau menghasilkan kunci kriptografi yang sama selama setiap upaya autentikasi. Ini setara dengan tingkat ketidakcocokan palsu dari sistem biometrik. Di sisi lain, menyimpan informasi yang lebih redundan dalam bentuk data pembantu memperkenalkan dua masalah utama. Pertama, toleransi kesalahan yang lebih besar biasanya akan menghasilkan tingkat kecocokan palsu yang lebih tinggi. Kedua, sketsa aman yang lebih besar pasti akan mengungkapkan lebih banyak informasi tentang fitur biometrik dan kunci kriptografi. Oleh karena itu, baik keamanan templat biometrik dan entropi kunci kriptografi yang dihasilkan menurun. Mirip dengan kasus transformasi fitur yang tidak dapat dibalik, ada tradeoff antara keamanan templat biometrik dan kinerja pengenalan dalam kriptosistem biometrik.

Kriptografi biometrik pengikatan kunci:

Dalam kriptografi pengikatan kunci, templat biometrik diamankan dengan mengikatnya secara monolitik dengan kunci rahasia dalam kerangka kriptografi. Seperti yang ditunjukkan pada Gambar 7.20, satu entitas yang menyematkan kunci dan templat disimpan dalam basis data sebagai sketsa aman. Sketsa aman ini tidak mengungkapkan banyak informasi tentang kunci atau templat biometrik, yaitu, secara komputasi sulit untuk mendekode kunci atau templat tanpa pengetahuan tentang data biometrik pengguna. Pencocokan dalam sistem pengikatan kunci melibatkan pemulihan kunci dari data pembantu menggunakan fitur biometrik kueri dan memverifikasi validitas kunci.

Biasanya, data pembantu adalah asosiasi kode koreksi kesalahan (yang diindeks oleh kunci rahasia) dan templat biometrik. Ketika kueri biometrik berbeda dari templat dalam toleransi kesalahan tertentu, kata kode terkait dengan jumlah kesalahan yang sama dapat dipulihkan. Kata kode dengan kesalahan ini dapat didekode untuk mendapatkan kata kode yang tepat dan dengan demikian, memulihkan kunci yang disematkan. Pemulihan kunci yang benar menyiratkan kecocokan yang berhasil. Toleransi terhadap variasi intra-pengguna dalam data biometrik ditentukan oleh kemampuan koreksi kesalahan dari kata sandi terkait. Selain itu, pencocokan tidak langsung berdasarkan skema koreksi kesalahan menghalangi penggunaan pencocok canggih yang dikembangkan secara khusus untuk mencocokkan templat biometrik asli. Hal ini mungkin dapat menyebabkan pengurangan akurasi pencocokan. Salah satu kriptosistem biometrik pengikatan kunci yang paling awal dan paling terkenal adalah skema komitmen fuzzy. Skema ini dapat diterapkan pada sistem biometrik di mana vektor fitur adalah string biner dengan panjang tetap.

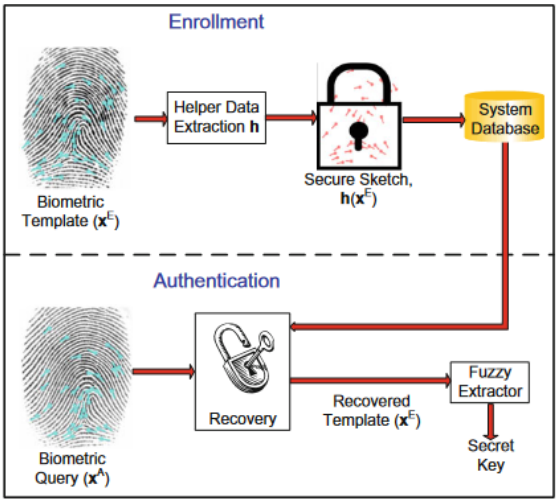


Gambar 7.20 Mekanismen Autentikasi Ketika Templat Biometric Diamankan Menggunakan Sistem Kriptografi Biometrik Pengikat Kunci

Misalkan templat pendaftaran X^E adalah string biner dengan panjang d bit. Selama pendaftaran, kata sandi koreksi kesalahan c dengan panjang yang sama $(d\ bit)$ dipilih. Kata sandi ini diindeks secara unik oleh kunci rahasia κ dengan panjang m bit (ada korespondensi satu-satu antara c dan κ). Di sini, m lebih kecil dari d dan parameter $(d - m)$ adalah ukuran redundansi dalam kode koreksi kesalahan. Kata kode c kemudian dikomit (diikat) ke vektor fitur biometrik X^E untuk menghasilkan sketsa aman. Sketsa aman atau data pembantu terdiri dari komitmen fuzzy ($X^E \oplus$ c) dan g(κ), di mana $g(.)$ adalah fungsi hash kriptografi dan $\oplus$ mewakili operasi eksklusif-atau (XOR) (penambahan modulo-2). Selama autentikasi, pengguna menyajikan vektor biometrik X^A. Sekarang seseorang dapat menghitung kata kode dengan kesalahan, c', sebagai c' = $X^A \oplus (X^E \oplus$ c). Jika X^A dekat dengan X^E, c' dekat dengan c karena $X^E \oplus$ xE = c' $\oplus$ c. Oleh karena itu, c' sekarang dapat didekodekan untuk mendapatkan kata kode terdekat c^*., yang akan sama dengan c asalkan jarak antara c dan c' kurang dari kapasitas koreksi kesalahan kode. Dari c^*., kita dapat menghitung K^*. Pencocokan berhasil jika g(K^*.)= g(K).

Kriptografi biometrik pembangkit kunci:

Pembuatan kunci kriptografi langsung dari biometrik merupakan usulan yang menarik, tetapi merupakan masalah yang sulit karena dua alasan: (a) variabilitas intra-pengguna dari fitur biometrik, dan (b) sifat distribusi probabilitas fitur biometrik yang tidak seragam. Konsep sketsa aman atau data pembantu dapat digunakan untuk memecahkan masalah pertama. Dalam skenario ini, sketsa aman diperoleh hanya menggunakan templat biometrik dan mekanisme pemulihan memfasilitasi rekonstruksi templat yang tepat saat disajikan dengan kueri yang dekat dengan templat seperti yang diilustrasikan dalam Gambar 7.21. Skema pembuatan kunci biometrik awal menggunakan skema kuantisasi khusus pengguna. Informasi tentang batas kuantisasi disimpan sebagai data pembantu, yang digunakan selama autentikasi untuk memperhitungkan variasi intra-pengguna. Dimungkinkan juga untuk menggunakan skema pengodean koreksi kesalahan untuk menghasilkan sketsa aman dari fitur biometrik.



Gambar 7.21 Mekanisme Autentikasi Saat Templat Biometrik Diamankan Menggunakan Kriptosistem Biometrik Pembangkit Kunci.

Kriptografi tradisional juga mengharuskan kunci kriptografi memiliki distribusi acak yang seragam. Akan tetapi, sudah diketahui umum bahwa fitur biometrik tidak terdistribusi secara seragam. Ekstraktor fuzzy diusulkan sebagai primitif kriptografi yang menghasilkan kunci kriptografi acak yang seragam dari fitur biometrik. Sketsa aman merupakan komponen integral dari ekstraktor fuzzy, yang mengatasi masalah stabilitas kunci. Masalah ketidakseragaman dapat ditangani dengan menerapkan fungsi hash kriptografi pada templat biometrik. Ingat kembali bahwa fungsi hash kriptografi memiliki sifat-sifat yang diinginkan seperti ketahanan pra-gambar dan ketahanan benturan. Sifat-sifat ini memfasilitasi ekstraksi string biner acak yang seragam dari fitur biometrik.

Pembahasan Tentang Skema Keamanan Templat

Ringkasan singkat dari berbagai pendekatan perlindungan templat biometrik disajikan dalam Tabel 7.1. Selain enkripsi standar dan skema transformasi fitur yang dapat dibalik, tidak ada skema perlindungan templat lainnya yang memerlukan informasi rahasia (seperti kunci) yang harus disimpan atau disajikan dengan aman selama pencocokan. Selain itu, banyak teknik perlindungan templat yang diusulkan dalam literatur menggunakan lebih dari satu pendekatan dasar (misalnya, transformasi yang dapat dibalik, diikuti oleh pengikatan kunci). Skema hibrida semacam itu belum dibahas secara rinci di sini.

Tabel 7.1 Ringkasan berbagai skema perlindungan templat. Di sini, X^E mewakili templat biometrik, X^A mewakili kueri yang disajikan selama autentikasi, dan κ adalah kunci (atau parameter) yang digunakan untuk melindungi templat atau dihasilkan dari templat. Dalam pendekatan transformasi fitur, f mewakili fungsi transformasi dan mt mewakili pencocok yang beroperasi di domain yang ditransformasikan. Dalam kriptosistem biometrik, h adalah skema ekstraksi data pembantu dan m adalah mekanisme pemulihan koreksi kesalahan yang memungkinkan rekonstruksi kunci κ.

Tabel 7.1 Ringkasan berbagai skema perlindungan templat

Mendekati	Fitur keamanan	Entitas yang disimpan	Mekanisme untuk menangani variasi intra pengguna
Transformasi	Kerahasiaan Kunci K	Domain Publik: yang di	Kuantitas dan

yang dapat dibalikkan		transformasikan templat $f(x^E, K)$ Rahasia: Kunci K	pencocokan dalam domain yang di transformasikan m_1 $(f(x^E,k), (f(x^A,k))$
Transformasi tak terbalik	Ketidakterbalikan fungsi transformasi	Domain Publik: yang di transformasikan templat $f(x^E, K)$ Rahasia: Kunci K	Pencocokan dalam domain transformasi m_t $(f(x^E,k), (f(x^A,k))$
Kriptografi biometrik pengikat kunci	Tingkat keamanan tergantung pada jumlah informasi yang diungkap oleh pembantu **H**	Domain Publik: data pembantu $H=h(x^E, K)$	Koreksi kesalaham dan kuantifikasi spesifik pengguna $K = m(f(x^E,k),x^A)$
Sistem kriptografi biometrik pembangkit kunci	Tingkat keamanan tergantung pada jumlah informasi yang diungkap oleh data pembantu **H**	Domain Publik: data pembantu $H=h(x^E)$	Koreksi kesalahan dan kuantifikasi spesifik pengguna $K = m(h(x^E), X^A)$

Hingga saat ini, belum ada pendekatan "terbaik" untuk perlindungan templat yang sepenuhnya memenuhi semua persyaratan yang disebutkan. Skenario dan persyaratan aplikasi memainkan peran utama dalam pemilihan skema perlindungan templat. Misalnya, dalam aplikasi verifikasi biometrik seperti ATM bank, skema transformasi fitur yang dapat dibalikkan sederhana berdasarkan PIN pengguna mungkin cukup untuk mengamankan templat biometrik jika diasumsikan bahwa templat yang ditransformasikan dan PIN pengguna tidak akan dikompromikan secara bersamaan.

Di sisi lain, dalam aplikasi daftar pantauan bandara, transformasi yang tidak dapat dibalikkan adalah pendekatan yang lebih cocok karena menyediakan keamanan templat dan kemampuan untuk dibatalkan tanpa bergantung pada masukan lain dari pengguna. Kriptosistem biometrik lebih tepat dalam aplikasi pencocokan pada kartu karena sistem tersebut biasanya merilis kunci ke aplikasi terkait untuk menunjukkan pencocokan yang berhasil. Faktor utama lain yang memengaruhi pilihan skema perlindungan templat adalah ciri biometrik spesifik yang akan digunakan, representasi fiturnya, dan tingkat variasi intra-pengguna. Secara umum, lebih dari satu skema perlindungan templat dapat diterima dan pilihan pendekatan yang sesuai dapat didasarkan pada sejumlah faktor seperti kinerja pengenalan, kompleksitas komputasi, persyaratan memori, dan penerimaan serta kerja sama pengguna. Penelitian lebih lanjut di bidang keamanan templat biometrik diharapkan akan berkembang di sepanjang tiga arah utama berikut:

1. Apa fungsi transformasi fitur atau teknik pembuatan sketsa yang "optimal" untuk jenis fitur biometrik dan fungsi pencocokan tertentu? Optimalitas umumnya mengacu pada pertukaran terbaik antara keamanan dan kinerja pengenalan. Beberapa representasi fitur utama mencakup string biner dengan panjang tetap (misalnya, IrisCode), set yang tidak berurutan (misalnya, detail sidik jari), dan vektor

bernilai riil dengan panjang tetap (misalnya, fitur LDA yang berasal dari gambar wajah). Representasi fitur ini mungkin juga memerlukan fungsi pencocokan yang berbeda seperti jarak Hamming, metrik perbedaan set, jarak edit, dll. Bergantung pada jenis fitur dan fungsi pencocokan, pendekatan keamanan templat yang sesuai dapat bervariasi.

2. Misalkan ada algoritme perlindungan templat yang baik untuk jenis fitur dan fungsi pencocokan tertentu; apa cara terbaik untuk menanamkan jenis fitur lain dalam domain fitur yang diinginkan? Misalnya, sebagian besar skema koreksi kesalahan dapat dengan mudah diterapkan untuk pembuatan sketsa aman dari string biner. Oleh karena itu, akan bermanfaat untuk mengubah jenis fitur lain, misalnya set detail sidik jari, menjadi string biner sehingga algoritme sketsa aman yang ada dapat digunakan. Pertanyaan ini juga relevan jika ada kebutuhan untuk mengamankan templat dari beberapa ciri biometrik sebagai satu kesatuan.
3. Terakhir, salah satu tugas penting tetapi sulit dalam desain algoritma perlindungan templat adalah: bagaimana perancang sistem mengukur keamanan yang disediakan oleh algoritma? Sebagian besar metodologi yang ada untuk analisis keamanan didasarkan pada asumsi yang tidak realistis (misalnya, distribusi seragam ciri biometrik). Masalah terkait adalah kebutuhan untuk mengukur entropi inheren dalam (atau individualitas) ciri biometrik atau ciri yang diekstraksi darinya.

RINGKASAN

Dengan penerapan sistem biometrik dalam skala besar di berbagai aplikasi komersial dan pemerintah, masalah keamanan yang terkait dengan sistem biometrik itu sendiri menjadi semakin penting. Sistem biometrik rentan terhadap sejumlah ancaman keamanan seperti intrusi, penolakan layanan, penolakan, dan penyerobotan fungsi. Analisis sistematis terhadap ancaman ini sangat penting saat merancang sistem biometrik. Bab ini menyajikan kategorisasi tingkat tinggi dari berbagai kerentanan sistem biometrik dan membahas tindakan pencegahan yang telah diusulkan untuk mengatasi ancaman ini.

Catatan Bibliografi Dan Historis

Karena pertumbuhan pesat dalam teknologi penginderaan dan komputasi, sistem biometrik telah menjadi bagian integral dari manajemen identitas modern dan sistem keamanan teknologi informasi (TI). Tentu saja, identifikasi potensi kerentanan dalam sistem biometrik telah mendapat perhatian yang meningkat dari komunitas penelitian biometrik. Sejumlah penelitian telah menganalisis potensi pelanggaran keamanan dalam sistem biometrik dan mengusulkan metode untuk melawan pelanggaran tersebut metode formal analisis kerentanan seperti pohon serangan juga telah digunakan untuk mempelajari bagaimana keamanan sistem biometrik dapat dikompromikan.

Titik-titik serangan dalam sistem biometrik diidentifikasi dalam Serangan pada antarmuka pengguna karena penyajian sifat biometrik palsu dipelajari dalam sejumlah upaya telah dilakukan dalam mengembangkan solusi perangkat keras maupun perangkat lunak yang mampu melakukan deteksi keaktifan. Juels menguraikan masalah keamanan dan

privasi yang diperkenalkan oleh saluran komunikasi yang tidak aman dalam aplikasi e-paspor yang menggunakan autentikasi biometrik. Saluran komunikasi yang tidak aman juga memungkinkan penyerang untuk meluncurkan serangan replay atau hill-climbing . Penanggulangan terhadap serangan replay dan hill-climbing meliputi stempel waktu dan mekanisme tantangan/respons. Kriptografi biometrik awalnya dikembangkan untuk tujuan mengamankan kunci kriptografi menggunakan fitur biometrik atau secara langsung menghasilkan kunci kriptografi dari fitur biometrik. Salah satu referensi paling awal untuk kriptografi biometrik adalah paten yang dikeluarkan untuk Albert Bodo pada tahun 1994 yang menjelaskan teknik untuk menggunakan templat biometrik sebagai kunci kriptografi. Dimulai pada tahun 1998, skema perlindungan templat praktis mulai muncul dalam literatur. Soutar merancang teknik yang mengaitkan kunci eksternal dengan data biometrik. Sistem tersebut secara efektif memastikan pemulihan kunci terkait ketika gambar biometrik yang cocok disajikan selama autentikasi bahkan dengan adanya variasi intra-kelas. Davida merancang teknik menggunakan kode koreksi kesalahan untuk mengamankan templat biometrik yang disimpan dalam kartu pintar dalam sistem autentikasi off-line.

Komitmen fuzzy dan brankas fuzzy adalah dua teknik paling populer yang digunakan untuk membangun kriptosistem biometrik. Implementasi praktis dari kedua skema ini telah diusulkan untuk ciri biometrik umum seperti sidik jari dan iris. Skema perlindungan templat yang diusulkan dalam adalah contoh kriptosistem biometrik hibrida. Pembuatan kunci kriptografi langsung dari biometrik merupakan usulan yang menarik tetapi merupakan masalah yang sulit karena variabilitas intra-pengguna. Dodis memperkenalkan konsep sketsa aman dan ekstraktor fuzzy dalam konteks pembuatan kunci dari biometrik. Sutcu. membahas masalah praktis dalam konstruksi sketsa aman dan mengusulkan sketsa aman berdasarkan kuantisasi untuk biometrik wajah. Masalah pembuatan ekstraktor fuzzy dari distribusi kontinu ditangani oleh Buhan . Protokol untuk autentikasi aman dalam aplikasi jarak jauh juga telah diusulkan berdasarkan skema ekstraktor fuzzy. Kriptografi biometrik menawarkan perlindungan terhadap pemulihan templat biometrik asli jika penyerang memperoleh akses ke basis data sistem. Namun, pendekatan ini memberikan perlindungan yang sangat terbatas terhadap pencocokan silang templat biometrik di berbagai basis data. Untuk mengatasi masalah ini, teknik transformasi templat dirancang.

Teknik-teknik ini secara permanen mendistorsi data biometrik menggunakan beberapa data khusus pengguna sambil mempertahankan atau bahkan meningkatkan kapasitas pengenalan sistem biometrik. Ratha mengusulkan teknik pertama untuk mendistorsi gambar wajah atau sidik jari menggunakan kunci khusus pengguna. Beberapa tahun kemudian, sejumlah teknik lain diusulkan untuk berbagai modalitas biometrik seperti sidik jari wajah, dan iris. Karena kinerja pencocokan merupakan salah satu persyaratan utama sistem pengenalan biometrik, maka diinginkan untuk mencapai kinerja yang baik bahkan ketika teknik perlindungan templat biometrik diterapkan. Teknik-teknik dirancang dengan menggabungkan fitur-fitur tambahan dari ciri biometrik yang sama dalam kriptosistem atau menggabungkan beberapa ciri biometrik dalam templat yang sama. Ada minat alami di antara para peneliti untuk memperkirakan tingkat keparahan ancaman

terhadap templat biometrik dan efektivitas teknik-teknik yang diusulkan dalam mengurangi risiko tersebut. Sejumlah teknik telah dikembangkan untuk menunjukkan bahwa sidik jari dapat direkonstruksi menggunakan templat yang tersimpan. Teknik-teknik lain diusulkan untuk secara eksplisit memperkirakan konten informasi (atau variabilitas di seluruh populasi) dalam ciri-ciri biometrik. Teknik-teknik juga diusulkan untuk mengevaluasi kemampuan keamanan yang disediakan oleh berbagai teknik.

Baik kriptosistem biometrik maupun teknik transformasi templat tidak bersifat double-blind, yaitu, sistem biometrik biasanya mengetahui pengguna mana yang sedang diautentikasi dalam transaksi tertentu, sementara pengguna tidak tahu apakah ia berinteraksi dengan sistem biometrik yang sah. Untuk mengatasi keterbatasan ini, teknik dan protokol autentikasi baru berdasarkan enkripsi homomorfik telah diusulkan baru-baru ini. Meskipun penelitian signifikan, perbaikan lebih lanjut terhadap teknik perlindungan templat diperlukan baik dari segi kinerja pencocokan dan keamanan sebelum dapat digunakan dalam sistem biometrik praktis.

DAFTAR PUSTAKA

A. K. Jain, K. Nandakumar, & A. Ross (2016). *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*. *Pattern Recognition Letters*, 79, 80-89.

A. K. Jain, R. Bolle, & S. Prabhakar (2009). *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers.

A. Ross & A. K. Jain (2003). *Information Forensics and Security: From Theory to Practice*. IEEE Transactions on Information Forensics and Security, 1(1), 1-7.

C. H. Lee & T. J. Chang (2011). *Biometric Authentication: A Review of Recent Advances*. *International Journal of Computer Applications*, 34(10), 1-6.

D. D. Y. O. Santos & T. A. O. Silva (2016). *Biometrics: A New Approach to Personal Identification*. *Journal of Information Security and Applications*, 26, 123-130.

D. Maltoni, D. Maio, A. K. Jain, & M. Ferrara (2009). *Handbook of Fingerprint Recognition*. Springer.

Gupta, R. K., Tiwari, A. G. P., & Jain, P. K. (2017). *Recent Advances in Biometric Systems: A Review*. *International Journal of Engineering and Technology*, 9(2), 1151-1157.

J. Z. Wang, W. W. Zheng, & L. Y. Wang (2018). *Biometric Recognition: Challenges and Opportunities*. *IEEE Transactions on Information Theory*, 64(11), 7491-7500.

Jain, A. K., Bolle, R., & Prabhakar, S. (2006). *Biometrics: Personal Identification in Networked Society*. New York: Springer.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometrics*. Springer.

Jindal, A., & Singh, A. (2019). *Emerging Trends in Biometrics*. In *Proceedings of the International Conference on Advances in Computing, Communication and Control*.

K. Nandakumar, A. Ross, & A. K. Jain (2016). *50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities*. *Pattern Recognition Letters*, 79, 80-89.

Khamis, A. & Jabbar, M. (2017). *Biometric Systems: From Theory to Practice*. Wiley.

Lee, C. H., & Chang, T. J. (2011). *A Survey of Biometric Authentication*. *International Journal of Computer Applications*, 34(10), 1-6.

Maltoni, D., Maio, D., Jain, A. K., & Ferrara, M. (2009). *Handbook of Fingerprint Recognition*. Springer.

Maltoni, D., Maio, D., Jain, A. K., & Ferrara, M. (2009). *Handbook of Fingerprint Recognition*. New York: Springer.

N. K. Ratha & R. M. Bolle (2004). *Biometric Systems: Design and Performance Evaluation*. Springer.

P. L. T. D. Hu & Y. Y. Zhang (2020). *Biometric Systems: A Comprehensive Overview*. *Journal of Computer Science and Technology*, 35(4), 799-815.

P. L. T. D. Hu, & Y. Y. Zhang (2020). *Biometric Authentication: Key Technologies and Applications*. *Journal of Information Security and Applications*, 26, 123-130.

R. K. Gupta, A. G. P. Tiwari, & P. K. Jain (2017). *Biometric Authentication: A Review of Key Technologies*. *International Journal of Engineering and Technology*, 9(2), 1151-1157.

Raghavendra, R., & Bhatia, M. (2015). *Biometric Recognition: Challenges and Opportunities*. *IEEE Transactions on Information Forensics and Security*, 10(4), 753-760.

Ratha, N. K., & Bolle, R. (2004). *Biometric Systems: Design and Performance Evaluation*. New York: Springer.

Ratha, N. K., Frankel, R., & Bolle, R. (2001). *Automatic Fingerprint Recognition Systems*. Springer.

Ross, A. & Jain, A. K. (2006). *Multimodal Biometrics: An Overview*. In *Biometrics: Theory, Methods, and Applications*. Springer.

Ross, A., & Jain, A. K. (2004). *Multimodal Biometrics: An Overview*. In *Proceedings of the 4th International Conference on Biometrics*. Berlin: Springer.

Schmid, C., & Tzeng, J. (2008). *Biometrics: A Very Short Introduction*. Oxford University Press.

Wayman, J. L., Hicklin, R. A., & Nanavati, S. (2005). *Biometric Systems: Technology, Design, and Performance Evaluation*. Springer.

Wu, J., & Yan, Y. (2011). *Biometric Recognition: Security and Privacy Concerns*. Journal of Computer Security, 19(2), 151-175.

Y. Y. Zhang, & K. Nandakumar (2018). *Biometric Systems: A Comprehensive Overview*. *Journal of Computer Science and Technology*, 35(4), 799-815.

Zhuang, Y., & Chen, X. (2012). *Introduction to Biometric Authentication*. In *Advances in Biometrics*. Springer.

BIOMETRIK DAN SISTEM SEKURITI

Dr. Joseph Teguh Santoso, S.Kom, M.Kom.

BIODATA PENULIS

Dr. Joseph Teguh Santoso, M.Kom adalah pemimpin yang visioner dan praktisi industri berpengalaman, yang menjabat sebagai Rektor Universitas Sains dan Teknologi Komputer (Universitas STEKOM), salah satu universitas terkemuka di Jawa Tengah, Indonesia. Dengan pengalaman lebih dari 13 tahun di dunia bisnis dan praktisi industri di China, beliau membawa perspektif global dan inovasi yang signifikan ke dalam dunia akademis.Sebagai seorang entrepreneur, penulis adalah pencipta TopLoker.com, sebuah platform inovatif yang merevolusi cara mencari dan menawarkan pekerjaan. TopLoker.com adalah portal lowongan bursa kerja terbesar di Indonesia, khusus untuk pendidikan SMA/SMK sederajat. TopLoker.com telah mendapatkan penghargaan sebagai juara 1 Startup4industry 2022 oleh Kementerian Perindustrian Republik Indonesia. Kontribusi Dr. Joseph dalam menyediakan akses pekerjaan yang luas bagi lulusan SMA/SMK telah membantu banyak individu menemukan peluang kerja yang sesuai dengan keahlian mereka. Selain itu, Dr. Joseph Teguh Santoso, M.Kom adalah pendiri dari dua organisasi yaitu (1) organisasi guru/pendidik PTIC (Perkumpulan Teacherpreneur Indonesia Cerdas) yang bertujuan untuk meningkatkan kualitas pendidikan dan kesejahteraan guru/pendidik dengan wawasan entrepreneurship, serta (2) organisasi industri PERKIVI (Perkumpulan Komunitas Industri dan Vokasi Indonesia) yang berfokus pada pengembangan link and match antara industri dan dunia pendidikan. Sebagai Rektor, Dr. Joseph Teguh Santoso, M.Kom memiliki kepemimpinan yang berorientasi pada hasil, dan berkomitmen untuk mendorong kemajuan Universitas Sains dan Teknologi Komputer (Universitas STEKOM). Saat ini Universitas STEKOM telah mengalami transformasi positif dalam peningkatan kualitas pendidikan, perluasan fasilitas, serta penguatan kemitraan Perguruan Tinggi Nasional dan Internasional. Beliau memprioritaskan pengembangan sumber daya manusia dan penelitian, serta memastikan bahwa universitas berada di garis depan dalam inovasi dan teknologi untuk mencapai tujuan akhir, yaitu lulusan yang mampu bekerja dan sukses setelah lulus.Dr. Joseph Teguh Santoso, M.Kom sering diundang sebagai pembicara di berbagai konferensi nasional maupun internasional dan telah menerima berbagai penghargaan atas dedikasinya dalam bidang pendidikan, industri, dan kewirausahaan.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

ISBN 978-623-8642-48-9 (PDF)