

BAB II

TEKNOLOGI BIOMETRIK DALAM SISTEM MODERN

A. Definisi Teknologi Biometrik

Biometrik berasal dari kata “*bios*” yang berarti hidup dan “*matric*” yang berarti pengukuran. Secara harfiah, biometrik adalah pengukuran dan analisis karakteristik biologis atau perilaku individu. Karakteristik ini kemudian digunakan untuk mengidentifikasi atau memverifikasi identitas seseorang. Contoh karakteristik biometrik meliputi sidik jari, wajah, iris mata, suara, dan banyak lagi.¹

Biometrik adalah teknologi yang mengidentifikasi dan memverifikasi individu berdasarkan karakteristik fisik atau perilaku unik mereka. Data biometrik bisa mencakup sidik jari, pengenalan wajah, iris mata, atau suara. Teknologi biometrik memanfaatkan keunikan karakteristik tersebut untuk mengenali individu dengan tingkat akurasi yang sangat tinggi.

Verifikasi biometrik adalah proses memverifikasi identitas seseorang dengan menggunakan karakteristik biologis, fisik, atau perilaku, seperti pemindaian wajah, gerakan, atau atribut unik lainnya, untuk tujuan keamanan digital. Sistem verifikasi identitas digital berbasis biometrik ini dirancang untuk memberikan verifikasi identitas yang akurat

¹ George Meletiou et al., “Design and Implementation of an E-Exam System Based on the Android Platform,” *Proceedings of the 2012 16th Panhellenic Conference on Informatics, PCI 2012* 14, no. 1 (2012): 375–80, <https://doi.org/10.1109/PCI.2012.76>.

dan mampu memastikan bahwa identitas seseorang dapat dibuktikan dengan tepat.²

Data yang digunakan dalam verifikasi biometrik bersifat pribadi dan tidak dapat dipalsukan oleh pihak lain. Berbeda dengan *password*, data biometrik tidak bisa dilupakan, hilang, atau mudah disalin. Setelah data biometrik tersimpan pada sistem sebuah aplikasi, pengguna hanya perlu melakukan pemindaian biometrik seperti selfie atau pemindaian sidik jari. Sistem akan membandingkan dan menganalisis apakah data biometrik pengguna cocok dengan data yang tersimpan. Jika cocok, sistem akan memberikan izin akses kepada pengguna.

Teknologi verifikasi biometrik modern memungkinkan proses verifikasi dilakukan secara digital dan otomatis. Teknik enkripsi yang digunakan dalam biometrik membuat data biometrik sulit untuk direplikasi oleh pihak luar, sehingga mencegah terjadinya pemalsuan atau pencurian data.

Biometrik menawarkan sejumlah kelebihan yang signifikan dalam keamanan dan otentikasi. Salah satunya adalah tingkat keamanan yang tinggi karena biometrik menggunakan karakteristik unik individu, seperti sidik jari atau wajah, yang sulit untuk ditiru atau dicuri. Selain itu, penggunaan biometrik juga memungkinkan proses otentikasi

² Basuki Supartono, "Regulasi Pelayanan Kesehatan Pada Penggunaan Aplikasi Biometrik," *Kementrian Kesehatan Indonesia* 3, no. 1 (2024): 1–19.

yang cepat dan mudah, mengurangi kebutuhan untuk mengingat kata sandi atau membawa kartu akses.³

Teknologi biometrik adalah metode identifikasi dan verifikasi identitas individu berdasarkan karakteristik biologis atau perilaku unik yang dimiliki oleh setiap orang. Karakteristik ini dapat berupa sidik jari, pola wajah, iris mata, suara, hingga bentuk telapak tangan. Teknologi biometrik semakin populer karena kemampuannya memberikan keamanan yang lebih tinggi dan kemudahan dalam berbagai sistem modern. Teknologi biometrik adalah metode identifikasi dan verifikasi identitas individu berdasarkan karakteristik biologis atau perilaku unik yang dimiliki oleh setiap orang. Karakteristik ini mencakup atribut fisik seperti sidik jari, pola wajah, iris mata, dan telapak tangan, serta karakteristik perilaku seperti suara dan pola pengetikan. Teknologi biometrik memberikan solusi yang lebih aman dan efisien dibandingkan dengan metode konvensional seperti penggunaan PIN atau password.

Pada intinya, biometrik memanfaatkan keunikan setiap individu yang tidak dapat dengan mudah disalin atau dipalsukan. Teknologi ini bekerja dalam dua tahap utama, pendaftaran *enrollment* dan verifikasi atau identifikasi. Selama proses pendaftaran, sistem akan menangkap data biometrik pengguna, seperti memindai sidik jari atau wajah,

³ Lixiang Li et al., "A Review of Face Recognition Technology, *IEEE Access* 8 (2020): 139110–20, <https://doi.org/10.1109/ACCESS.2020.3011028>.

yang kemudian dikonversi menjadi *template* digital yang disimpan secara aman. Dalam proses verifikasi, data biometrik yang baru diambil akan dibandingkan dengan *template* yang telah tersimpan untuk memastikan kesesuaian.⁴

Berikut adalah keunggulan dari penggunaan sistem verifikasi identitas berbasis biometrik:

1. Hanya Dimiliki Satu Orang

Verifikasi biometrik adalah sistem yang bersifat unik dan hanya dapat diakses oleh satu orang saja, karena setiap data verifikasi sangat pribadi dan tidak bisa dipalsukan oleh orang lain.

2. Kecepatan Dan Efisiensi Skala Masif

verifikasi biometrik modern memungkinkan verifikasi identitas dilakukan dalam skala besar dengan waktu yang sangat singkat. Inilah mengapa sistem ini digunakan oleh pemerintahan, perbankan, dan institusi finansial yang memerlukan keamanan tinggi tapi juga mudah dan cepat.

3. Tingkat Akurasi Yang Tinggi

Sistem verifikasi biometrik adalah sistem yang dapat mengenali seseorang dengan tepat, akurat, dan konsisten, sehingga mengurangi kesalahan dalam mengenali individu. Keamanan ini sangat penting untuk

⁴ S. Koteswari et al., "Fusion of Iris and Fingerprint Biometric Identifier for ATM Services: An Investigative Study," *International Journal of Communications, Network and System Sciences* 09, no. 11 (2016): 506–18, <https://doi.org/10.4236/ijcns.2016.911040>.

mencegah upaya pemalsuan.

4. Kemudahan Akses

Pengguna tidak perlu membawa alat verifikasi seperti kartu atau perangkat lainnya. Cukup dengan menunjukkan data biometrik yang melekat pada tubuh, verifikasi identitas dapat dilakukan.

5. Keamanan Yang Lebih Tinggi

Sistem verifikasi biometrik mengeliminasi risiko lupa kata sandi atau PIN. Karena data biometrik melekat pada diri seseorang, risiko pencurian akses juga berkurang.

6. Kemudahan Penggunaan

Verifikasi identitas menggunakan teknologi biometrik mudah dilakukan tanpa memerlukan *intervensi* atau pelatihan khusus, sehingga meminimalisir kesulitan akses.

7. Meningkatkan Akuntabilitas

Teknologi verifikasi biometrik mampu mencatat setiap aktivitas penggunaanya dengan lebih tepat dan akurat, meningkatkan akuntabilitas sistem keamanan yang dapat diandalkan.

8. Tahan Dari Kerusakan

Data biometrik tidak rentan terhadap kerusakan fisik seperti kartu yang bisa hilang, patah, atau terbakar, dipalsukan. Data biometrik tidak bisa digunakan ketika

pemilikinya sudah meninggal dunia.⁵

B. Jenis Teknologi Biometrik

1. Pengenalan Sidik Jari



Gambar 1.1 Sidik Jari

Pengenalan sidik jari adalah metode biometrik yang paling umum digunakan. Teknologi ini bekerja dengan memindai dan menganalisis pola unik pada ujung jari seseorang. Keunggulan metode ini terletak pada tingkat akurasi yang tinggi dan biaya implementasi yang relatif rendah.⁶

Pengenalan sidik jari adalah salah satu metode biometrik yang paling populer dan banyak digunakan dalam berbagai sistem keamanan dan layanan digital. Teknologi ini bekerja dengan memindai pola unik pada permukaan kulit ujung jari seseorang. Setiap individu memiliki pola sidik jari yang berbeda, bahkan pada kedua

⁵ Muhammad Naufal Afif and Mohammad Kemal Dermawan, "Penggunaan Alat Biometrik Sidik Jari Sebagai Kontrol Akses Dalam Analisis CPTED Terhadap Risiko Trespassing Di Instalasi Gudang Material Korporasi ' X ,'" *Akademika* 5, no. 4 (2024): 819–30.

⁶ "Handbook of Fingerprint Recognition," *Handbook of Fingerprint Recognition*, 2003, <https://doi.org/10.1007/b97303>.

tanggannya, sehingga menjadikannya alat identifikasi yang andal.⁷

Teknologi pengenalan sidik jari melibatkan pemindaian pola unik yang ada pada ujung jari seseorang. Proses identifikasi ini dimulai dengan pemindaian sidik jari, yang kemudian dibandingkan dengan pola yang tersimpan dalam database. Penggunaan sidik jari telah menjadi umum dalam berbagai aplikasi, mulai dari sistem keamanan perangkat seluler hingga akses ke fasilitas yang aman. Keunggulan utama teknologi ini adalah tingkat akurasi yang tinggi dan kemudahan penggunaannya. Namun, kekurangannya termasuk risiko pemalsuan melalui sidik jari palsu dan potensi kegagalan identifikasi jika jari pengguna kotor atau terluka.⁸

a. Cara Kerja Pengenalan Sidik Jari

1. Pendaftaran (*Enrollment*):

- a) Pengguna menempatkan jarinya pada pemindai sidik jari.

⁷ Anil Jain and Ajay Kumar, "Biometric Recognition: An Overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, vol. 11, 2012, 49–79, https://doi.org/10.1007/978-94-007-3892-8_3.

⁸ Alex Andrew, "GUIDE TO BIOMETRICS, by Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha and Andrew W. Senior Springer, New York, 2004, Hardback, Xxix+364 Pp., ISBN 0-387-40089-3 (£38.50) PRACTICAL BIOMETRICS: FROM ASPIRATION TO IMPLEMENTATION, by Ju," *Robotica* 22 (November 2004): 697–98, <https://doi.org/10.1017/S0263574704221130>.

- b) Sistem mengambil gambar pola sidik jari dan mengonversinya menjadi *template* digital yang tersimpan dalam basis data.
- b. Verifikasi:
 - a) Pengguna kembali menempatkan jarinya pada pemindai.
 - b) Sistem membandingkan pola sidik jari yang baru diambil dengan *template* yang tersimpan.
 - c) Jika cocok, akses diberikan; jika tidak, akses ditolak.
- c. Komponen Teknologi Pengenalan Sidik Jari
 - a. Sensor Sidik Jari: Bertugas menangkap pola sidik jari. Sensor ini dapat berupa optik, kapasitif, atau ultrasonik.
 - b. Algoritma Ekstraksi Fitur: Mengidentifikasi titik-titik karakteristik (*minutiae*) seperti bifurkasi dan *ridge endings*.
 - c. *Template Matching*: Membandingkan *template* sidik jari dengan data yang telah tersimpan.
- d. Keunggulan Pengenalan Sidik Jari
 - 1) Tingkat Akurasi Tinggi: Sidik jari sangat unik dan stabil seumur hidup.
 - 2) Cepat dan Efisien: Proses autentikasi hanya memerlukan beberapa detik.

- 3) Biaya Implementasi Rendah: Teknologi sensor sidik jari relatif murah dibandingkan teknologi biometrik lainnya.

e. Kelemahan Pengenalan Sidik Jari

- 1) Kerusakan Fisik: Luka atau bekas luka pada jari dapat mempengaruhi akurasi pemindaian.
- 2) Kepekaan Lingkungan: Sensor sidik jari mungkin tidak berfungsi optimal dalam kondisi jari yang basah atau kotor.
- 3) Risiko Pemalsuan: Meski sulit, sidik jari dapat dipalsukan dengan teknik tertentu.

f. Penerapan Dalam Sistem Modern

- a. Perangkat Seluler: Teknologi ini digunakan secara luas untuk membuka kunci perangkat dan melakukan pembayaran digital.
- b. Sistem Perbankan: Digunakan dalam mesin ATM dan layanan perbankan digital untuk autentikasi nasabah.
- c. Keamanan Gedung: Digunakan untuk mengontrol akses ke area dengan tingkat keamanan tinggi.

2. Pengenalan Wajah



Gambar 1.2 Pengenalan Wajah

Teknologi pengenalan wajah menggunakan algoritma canggih untuk menganalisis dan mencocokkan fitur wajah seseorang. Sistem ini sering digunakan dalam perangkat seluler dan sistem keamanan untuk identifikasi tanpa kontak. Teknologi pengenalan wajah menggunakan algoritma canggih untuk menganalisis dan mencocokkan fitur wajah seseorang. Sistem ini bekerja dengan memetakan berbagai titik wajah (*landmark points*), seperti jarak antara mata, bentuk hidung, dan kontur rahang. Data wajah yang diperoleh kemudian dikonversi menjadi *template* digital yang unik untuk setiap individu.⁹

⁹ Muhammad Andika Fadilla, Herri Setiawan, and Mustafa Ramadhan, "Implementasi Metode Convolutional Neural Network (Cnn) Pada Sistem Deteksi Emosi Dari Ekspresi Wajah Manusia Dengan Aplikasi Android Sebagai Antarmuka Pengguna," *Jurnal Ilmu Komputer Dan Sistem Informasi (JIKSI)* 9, no. 4 (2023): 126–38.

Pengenalan wajah merupakan teknologi biometrik yang menggunakan algoritma komputer untuk mengidentifikasi atau memverifikasi seseorang berdasarkan fitur wajah mereka. Cara kerjanya melibatkan pengambilan gambar wajah, yang kemudian dibandingkan dengan database gambar yang sudah ada. Aplikasi teknologi ini sangat luas, termasuk dalam keamanan perangkat seluler, kontrol akses ke gedung, dan sistem pengawasan publik. Keunggulan pengenalan wajah adalah kemampuannya untuk melakukan identifikasi tanpa kontak fisik, membuatnya lebih higienis dan nyaman bagi pengguna. Namun, kekurangan utamanya adalah masalah privasi dan potensi bias algoritma, yang bisa mengakibatkan kesalahan identifikasi terutama terhadap kelompok minoritas.¹⁰

a. Cara Kerja Teknologi Pengenalan Wajah

- 1) Deteksi Wajah: Sistem pertama-tama mendeteksi adanya wajah dalam gambar atau video.
- 2) Ekstraksi Fitur: Sistem memetakan fitur-fitur wajah yang relevan.

¹⁰ Matthew A. Turk and Alex P. Pentland, "Face Recognition Using Eigenfaces," 1991, <https://doi.org/10.5120/20740-3119>.

- 3) Pembuatan *Template*: Data fitur wajah dikonversi menjadi *template* digital.
- 4) Pencocokan *Template*: *Template* baru dibandingkan dengan data wajah yang tersimpan untuk verifikasi atau identifikasi.

b. Komponen Teknologi Pengenalan Wajah

- 1) Kamera: Digunakan untuk menangkap gambar wajah. Kamera yang berkualitas tinggi dapat meningkatkan akurasi sistem.
- 2) Algoritma Ekstraksi Fitur: Mengidentifikasi dan memetakan fitur unik wajah.
- 3) Database *Template*: Menyimpan *template* wajah untuk proses verifikasi.

c. Keunggulan Pengenalan Wajah

- 1) Non-Kontak: Tidak memerlukan kontak langsung, sehingga lebih higienis.
- 2) Kecepatan Verifikasi: Proses identifikasi dapat dilakukan dengan cepat.
- 3) Mudah Diintegrasikan: Teknologi ini dapat diterapkan pada perangkat yang sudah memiliki kamera.

d. Kelemahan Pengenalan Wajah

- 1) Kualitas Gambar: Pencahayaan yang buruk dapat mempengaruhi akurasi.
- 2) Perubahan Fisik: Faktor seperti penggunaan kacamata, janggut, atau perubahan berat badan dapat mempengaruhi hasil identifikasi.
- 3) Privasi: Isu privasi menjadi perhatian karena data wajah dapat dikumpulkan tanpa sepengetahuan individu.

e. Penerapan Dalam Sistem Modern

- 1) Perangkat Seluler: Digunakan untuk membuka kunci perangkat dan verifikasi pembayaran digital.
- 2) Sistem Keamanan: Dipakai untuk pengawasan di tempat umum dan kontrol akses.
- 3) Perbankan: Digunakan dalam layanan mobile banking untuk autentikasi nasabah.
- 4) Bandara: Mempercepat proses verifikasi identitas penumpang.

3. Pengenalan Iris Mata



Gambar 1.3 Pengenalan Iris Mata

Pengenalan iris mata memanfaatkan pola unik pada iris mata setiap individu. Teknologi ini memiliki tingkat akurasi yang sangat tinggi dan sulit untuk dipalsukan. Namun, biaya implementasinya relatif mahal. Pengenalan iris mata adalah metode biometrik yang memanfaatkan pola unik pada iris mata setiap individu. Iris mata memiliki pola yang sangat kompleks dan stabil sepanjang hidup seseorang, menjadikannya salah satu metode identifikasi yang paling akurat.¹¹

a. Cara Kerja Teknologi Pengenalan Iris Mata

- 1) Pemindaian Mata: Kamera inframerah digunakan untuk menangkap gambar iris.
- 2) Ekstraksi Fitur: Sistem menganalisis pola unik pada iris, seperti lingkaran dan tekstur yang khas.
- 3) Pembuatan *Template*: Data iris dikonversi menjadi template digital.

¹¹ Citra Wajah, Fakultas Ilmu Komputer, and Universitas Sriwijaya, "79529-ID-Analisis-Perbandingan-Transformasi-Wavel" 5, no. 2 (2010).

- 4) Verifikasi: *Template* dibandingkan dengan data yang telah tersimpan.

b. Keunggulan Pengenalan Iris Mata

- 1) Tingkat Akurasi Sangat Tinggi: Sulit untuk dipalsukan.
- 2) Stabilitas Pola: Pola iris tidak berubah seumur hidup.
- 3) Keamanan Tinggi: Cocok untuk aplikasi keamanan tingkat tinggi.

c. Kelemahan Pengenalan Iris Mata

- 1) Biaya Tinggi: Peralatan yang dibutuhkan mahal.
- 2) Non-Kontak: Memerlukan jarak tertentu untuk pemindaian yang akurat.
- 3) Kenyamanan Pengguna: Beberapa orang merasa tidak nyaman dengan pemindaian mata.

d. Penerapan dalam Sistem Modern

- 1) Sistem Keamanan Tingkat Tinggi: Digunakan dalam fasilitas militer dan penelitian.
- 2) Bandara: Untuk verifikasi penumpang.
- 3) Perbankan: Dalam autentikasi nasabah untuk layanan premium.

4 . Pengenalan Suara



Gambar 1.4 Pengenalan Suara

Pengenalan suara menggunakan analisis karakteristik suara individu untuk identifikasi. Mekanismenya melibatkan perekaman suara, yang kemudian diproses dan dibandingkan dengan sampel suara yang ada di database. Teknologi ini sering digunakan dalam sistem keamanan telepon, asisten virtual, dan verifikasi identitas jarak jauh. Keunggulan dari pengenalan suara adalah kenyamanannya karena tidak memerlukan kontak fisik atau perangkat tambahan khusus. Namun, kekurangannya mencakup potensi masalah dengan akurasi dalam lingkungan yang bising dan risiko peniruan suara oleh orang lain.¹²

Pengenalan suara bekerja dengan menganalisis pola suara unik seseorang, termasuk intonasi dan frekuensi suara. Teknologi ini cocok untuk aplikasi yang membutuhkan interaksi suara, seperti layanan perbankan berbasis telepon. Teknologi pengenalan suara bekerja

¹² Mengke Yang and Rustam Shadiev, "Review of Research on Technologies for Language Learning and Teaching," *Open Journal of Social Sciences* 07, no. 03 (2019): 171–81, <https://doi.org/10.4236/jss.2019.73014>.

dengan menganalisis pola suara unik setiap individu, termasuk intonasi, frekuensi, dan ritme bicara. Teknologi ini digunakan dalam aplikasi yang membutuhkan interaksi suara.

a. Cara Kerja Teknologi Pengenalan Suara

- 1) **Perekaman Suara:** Sistem menangkap suara pengguna.
- 2) **Ekstraksi Fitur:** Sistem menganalisis karakteristik suara yang unik.
- 3) **Pembuatan *Template*:** Data suara dikonversi menjadi *template* digital.
- 4) **Verifikasi:** *Template* dibandingkan dengan data suara yang tersimpan.

b. Keunggulan Pengenalan Suara

- 1) **Non-Kontak:** Tidak memerlukan perangkat tambahan.
- 2) **Mudah Digunakan:** Cukup dengan berbicara untuk verifikasi.
- 3) **Cocok untuk Layanan Jarak Jauh:** Digunakan dalam layanan berbasis telepon.

c. Kelemahan Pengenalan Suara

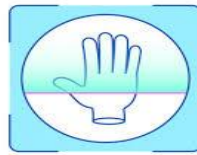
- 1) **Sensitif terhadap Lingkungan:** Suara bising dapat mempengaruhi akurasi.
- 2) **Perubahan Suara:** Faktor seperti flu atau kondisi emosional dapat mempengaruhi hasil.

- 3) Risiko Pemalsuan: Suara dapat direkam dan dipalsukan.

d. Penerapan Dalam Sistem Modern

- 1) Layanan Perbankan: Digunakan untuk verifikasi nasabah di layanan *call center*.
- 2) *Smart Home*: Untuk mengendalikan perangkat pintar.
- 3) Keamanan Akses: Dalam sistem
- 4) kontrol akses berbasis suara.

5. Pengenalan Telapak Tangan



Gambar 1.5 Pengenalan Telapak Tangan

Teknologi ini menggunakan pola vena dan bentuk telapak tangan untuk identifikasi. Pengenalan telapak tangan menawarkan keamanan yang tinggi karena sulit dipalsukan dan tetap efektif meskipun terdapat luka pada permukaan kulit.¹³

¹³ Rabia Jafri and Hamid Arabnia, "A Survey of Face Recognition Techniques," *JIPS* 5 (June 2009): 41–68, <https://doi.org/10.3745/JIPS.2009.5.2.041>.

Teknologi pengenalan telapak tangan menggunakan pola vena, garis, dan bentuk telapak tangan untuk identifikasi. Teknologi ini menawarkan keamanan yang tinggi karena pola vena sulit untuk dipalsukan.

a. Cara Kerja Teknologi Pengenalan Telapak Tangan

- 1) Pemindaian Telapak Tangan: Sistem menangkap gambar telapak tangan.
- 2) Ekstraksi Fitur: Analisis dilakukan terhadap pola vena dan struktur telapak tangan.
- 3) Pembuatan *Template*: Data telapak tangan dikonversi menjadi template digital.
- 4) Verifikasi: *Template* dibandingkan dengan data yang tersimpan.

b. Keunggulan Pengenalan Telapak Tangan

- 1) Tingkat Keamanan Tinggi: Sulit untuk dipalsukan.
- 2) Tidak Terpengaruh Luka: Pola vena tetap dapat terbaca meskipun ada luka di permukaan kulit.
- 3) Non-Kontak: Pemindaian dapat dilakukan tanpa menyentuh perangkat.

c. Kelemahan Pengenalan Telapak Tangan

- 1) Biaya Implementasi: Perangkat pemindai relatif mahal.
- 2) Ukuran Perangkat: Pemindai biasanya lebih besar dibandingkan sensor sidik jari.

d. Penerapan dalam Sistem Modern

- 1) Perbankan: Untuk verifikasi identitas nasabah di ATM.
- 2) Keamanan Gedung: Kontrol akses di area terbatas.
- 3) Fasilitas Kesehatan: Untuk identifikasi pasien.¹⁴

C. Perkembangan Teknologi Biometrik

Teknologi biometrik telah mengalami perkembangan pesat dalam beberapa dekade terakhir. Awalnya, teknologi ini hanya digunakan dalam lingkungan militer dan keamanan tinggi. Namun, dengan kemajuan teknologi digital dan kebutuhan akan sistem keamanan yang lebih baik, penerapan biometrik telah meluas ke berbagai sektor, termasuk perbankan, kesehatan, dan *e-commerce*. Inovasi seperti integrasi dengan kecerdasan buatan (AI) dan *blockchain* semakin meningkatkan efisiensi dan keamanan teknologi biometrik.¹⁵

Teknologi biometrik telah mengalami perkembangan pesat selama beberapa dekade terakhir. Teknologi ini memanfaatkan karakteristik unik manusia, baik fisik maupun

¹⁴ Ahmad Mardia, Iskandar Fitri, and Sari Ningsih, "Monitoring Sistem Biometrik Keamanan Laci Kasir Dengan Fingerprint Berbasis Android," *Jurnal JTIK (Jurnal Teknologi Informasi Dan Komunikasi)* 6 (January 2022): 378–85, <https://doi.org/10.35870/jtik.v6i3.426>.

¹⁵ Sumijan, Pradani Ayu, and Arlis Syafri, *Teknologi Biometrik Impementasi Pada Bidang Medis Menggunakan Matlabs, Teknologi Biometrik*, 2021.

perilaku, untuk identifikasi dan autentikasi. Berikut adalah perkembangan mendalam dalam teknologi biometrik:

1. Generasi Awal Teknologi Biometrik

Pada awalnya, teknologi biometrik hanya digunakan di lingkungan yang sangat terbatas seperti lembaga militer dan pemerintah untuk keperluan keamanan. Teknologi yang digunakan pada masa ini sederhana dan manual, contohnya:

- a. Sidik Jari Manual: Pemeriksaan sidik jari dilakukan secara visual oleh petugas.
- b. Pengenalan Wajah Dasar: Berdasarkan foto yang dicocokkan secara manual.

2. Otomasi Teknologi Biometrik (Era 1990-an)

Dengan berkembangnya komputasi, teknologi biometrik mulai beralih ke sistem otomatis. Beberapa perkembangan utama:

- a. Pemindai Sidik Jari Digital: Mulai digunakan secara luas di berbagai institusi keamanan dan penegakan hukum.
- b. Pengenalan Iris: Digunakan untuk keamanan tingkat tinggi, seperti pada pintu akses ke fasilitas sensitif.
- c. Pemrosesan Wajah Otomatis: Mulai dikembangkan untuk mendukung pengawasan di ruang publik.

3. Perkembangan Teknologi Biometrik di Abad ke-21

Dengan munculnya internet dan perangkat pintar, biometrik menjadi lebih luas diterapkan:

- a. Integrasi pada Perangkat Konsumen: Smartphone mulai dilengkapi dengan fitur pemindai sidik jari dan wajah.
- b. Teknologi Multimodal: Kombinasi berbagai biometrik (sidik jari, wajah, dan suara) untuk meningkatkan akurasi.
- c. Pemrosesan Data *Real-Time*: Teknologi kecerdasan buatan (AI) digunakan untuk mempercepat dan meningkatkan akurasi analisis biometrik.

4. Kemajuan Terkini (2020-an)

Teknologi biometrik semakin berkembang dengan dukungan AI, IoT, dan komputasi awan:

- a. Pemindai Wajah 3D: Teknologi yang lebih akurat dibandingkan pemindai 2D.
- b. Verifikasi Suara yang Lebih Canggih: Menggunakan pembelajaran mesin untuk memverifikasi suara meski ada gangguan latar belakang.
- c. Biometrik Perilaku: Menggunakan pola interaksi pengguna dengan perangkat, seperti pola mengetik dan gerakan kursor.
- d. Pemindaian Vena: Teknologi yang memanfaatkan pola pembuluh darah sebagai metode autentikasi yang sulit dipalsukan

5. Tantangan dan Isu Etika

Perkembangan teknologi biometrik membawa sejumlah tantangan:

- a. Privasi Data: Risiko penyalahgunaan data biometrik oleh pihak ketiga.
- b. Keamanan Data: Ancaman terhadap pencurian data biometrik yang tidak dapat diubah seperti kata sandi.
- c. Bias Algoritma: Kemungkinan bias pada algoritma biometrik yang dapat mendiskriminasi kelompok tertentu.

6. Masa Depan Teknologi Biometrik

- a. Peningkatan Keamanan Berbasis AI: AI akan terus meningkatkan kemampuan verifikasi biometrik.
- b. Biometrik Berbasis DNA: Teknologi yang masih dalam tahap penelitian.
- c. Integrasi *Blockchain* :Untuk memastikan keamanan dan anonimitas data biometrik.
- d. Penggunaan dalam *Metaverse*: Biometrik akan menjadi kunci autentikasi di dunia virtual.

Teknologi biometrik telah, dan akan terus, menjadi bagian penting dari kehidupan manusia. Dengan perkembangan yang terus maju, biometrik memiliki potensi untuk memberikan keamanan yang lebih baik dan

pengalaman pengguna yang lebih mulus di berbagai sektor industri.¹⁶



¹⁶ Fulan Yustinne et al., “Analisis Ancaman Cybercrime Dan Peran Sistem Biometrik : Systematic Literature Review,” *Cyber* 3, no. 1 (2023): 19–29.