Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika
Volume. 4 Nomor. 4 Juli 2026
e-ISSN: 3031-8912; p-ISSN: 3031-8904, Hal. 61-72
DOI: https://doi.org/10.61132/merkurius.v4i4.1318
Tersedia: https://journal.arteii.or.id/index.php/Merkurius

Analisis Keamanan Sistem Biometrik terhadap Ancaman *Deepfake*

(Studi Kasus Lonjakan 3.000% Fraud Incidents Periode 2023-2024)

Osewa Pallyama Sultan Khadir[1*], Asep Saeppani[2], Esa Firmansyah[3], Beben Sutara[4]
[1-4]Program Studi Informatika, Universitas Sebelas April Sumedang, Indonesia

**Penulis Korespondensi: 220660121046@student.unsap.ac.id*

Abstract. *The rapid advancement of deepfake technology powered by Generative AI has created a critical security threat to biometric authentication systems, particularly face recognition and voice recognition. Global reports from 2023-2024 indicate a dramatic 3,000% increase in deepfake-enabled identity fraud, emphasizing the urgent need for stronger biometric security measures. This study aims to analyze key vulnerabilities in biometric systems against deepfake attacks, evaluate the effectiveness of existing detection techniques, and develop a layered biometric security framework as a mitigation solution. The research employs a Systematic Literature Review (SLR) of scientific publications and industry reports from 2016-2025, complemented by Lite Expert Validation to assess the feasibility of the proposed framework. The findings reveal that most biometric systems remain vulnerable to advanced face swap, voice cloning, and liveness detection bypass attacks. Detection methods based on frequency–spatial analysis and multi-modal deepfake detection are identified as the most effective, although they require strong operational integration. This study introduces the Biometric Deepfake Security Framework, which incorporates technical, procedural, and adaptive security controls to enhance biometric resilience against digital identity manipulation. The proposed framework is expected to provide practical guidance for organizations relying on biometric authentication to strengthen protection against evolving deepfake threats.*

Keywords: *Biometrics; Cybersecurity; Deepfake; Face Recognition; Security Framework.*

Abstrak. Perkembangan teknologi *deepfake* berbasis Generative AI telah menimbulkan ancaman signifikan terhadap sistem autentikasi biometrik, khususnya pada face recognition dan voice recognition. Laporan global periode 2023-2024 menunjukkan lonjakan hingga 3.000% kasus penipuan identitas berbasis *deepfake*, menandakan perlunya evaluasi keamanan biometrik yang lebih komprehensif. Penelitian ini bertujuan menganalisis kerentanan utama pada sistem biometrik terhadap serangan *deepfake*, mengkaji efektivitas metode deteksi yang tersedia, serta menghasilkan sebuah *framework* keamanan berlapis sebagai solusi mitigasi. Metode penelitian menggunakan *Systematic Literature Review* (SLR) terhadap publikasi ilmiah dan laporan industri tahun 2016-2025, dilengkapi *Lite Expert Validation* untuk menilai kelayakan *framework*. Hasil penelitian menunjukkan bahwa sebagian besar sistem biometrik masih rentan terhadap serangan *face swap, voice cloning,* dan *bypass liveness detection* generasi terbaru. Metode deteksi berbasis analisis frekuensi-spasial dan multi-modal *detection* dinilai paling efektif namun membutuhkan integrasi operasional yang kuat. Penelitian ini menghasilkan Biometric *Deepfake Security Framework* yang mencakup kontrol teknis, prosedural, dan adaptif untuk meningkatkan ketahanan sistem biometrik terhadap manipulasi identitas digital. *Framework* ini diharapkan dapat menjadi acuan bagi industri dan lembaga yang menggunakan autentikasi biometrik dalam meningkatkan keamanan dari ancaman *deepfake* yang terus berkembang.

Kata kunci: Biometrik; *Deepfake*; *Framework* Keamanan; Keamanan Siber; Pengenalan Wajah.

1. LATAR BELAKANG

Perkembangan teknologi kecerdasan buatan *(Artificial Intelligence/AI),* khususnya generative AI, telah mendorong munculnya bentuk ancaman baru berupa *deepfake*, yaitu manipulasi wajah dan suara yang dihasilkan secara sintetis dengan tingkat realisme tinggi. Kemampuan *deepfake* yang semakin canggih menjadikannya alat berbahaya dalam serangan siber modern, terutama dalam konteks penipuan identitas *(identity fraud)* dan penyusupan terhadap sistem autentikasi biometrik.

Naskah Masuk: 16 April 2026; Revisi: 15 Mei 2026; Diterima: 28 Juni 2026; Terbit: 04 Juli 2026

Kasus global seperti penipuan berbasis *deepfake* yang menimpa perusahaan Arup dengan kerugian mencapai US$25 juta pada tahun 2024 menunjukkan bahwa serangan ini tidak lagi bersifat eksperimental, tetapi telah digunakan secara masif untuk tujuan kriminal. Laporan Sumsub (2024) bahkan mencatat peningkatan hingga 3.000% kasus penipuan identitas yang memanfaatkan teknologi *deepfake* dalam kurun waktu 2023-2024, sekaligus menegaskan urgensi persoalan ini.

Sistem autentikasi biometrik seperti *face recognition* dan *voice recognition* sebelumnya dianggap lebih aman dibandingkan kata sandi tradisional. Namun, penelitian terbaru menunjukkan bahwa kemampuan *deepfake* modern-yang dapat meniru ekspresi mikro, pergerakan mata, hingga pola suara secara *real-time*-membuat sebagian besar mekanisme biometrik rentan ditembus. Studi Ayeswarya & Singh (2024) dan He et al. (2024) mengungkapkan bahwa *liveness detection* dasar yang diterapkan pada banyak platform belum mampu menangani serangan *deepfake* generasi terbaru. Ancaman ini berdampak serius bagi sektor finansial, pemerintahan, e-KYC, hingga layanan digital yang bergantung pada autentikasi biometrik sebagai metode verifikasi utama.

Berbagai penelitian telah mengembangkan pendekatan deteksi *deepfake*, seperti analisis frekuensi-spasial, multi-modal *detection,* hingga arsitektur AI berbasis *deep learning.* Namun, sebagian besar pendekatan tersebut masih berfokus pada aspek teknis dan belum menjawab kebutuhan implementasi keamanan biometrik secara menyeluruh. Industri keamanan informasi seperti ISACA (2024) menekankan pentingnya sebuah *framework* keamanan yang bersifat holistik, menggabungkan deteksi teknis, kontrol prosedural, mitigasi risiko, serta edukasi pengguna.

Berdasarkan fenomena tersebut, penelitian ini dilakukan dengan tujuan menyusun sebuah *framework* solusi keamanan biometrik yang mampu memitigasi ancaman *deepfake* melalui analisis menyeluruh terhadap jenis serangan, kerentanan sistem biometrik, dan efektivitas metode deteksi yang ada. Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) dan validasi ahli untuk menghasilkan rekomendasi yang aplikatif dan dapat digunakan oleh berbagai sektor industri. Hasil penelitian ini diharapkan dapat memperkuat sistem autentikasi biometrik, menjawab gap penelitian yang masih ada, serta juga memberikan kontribusi nyata dalam meningkatkan keamanan identitas digital di era *generative* AI.

2. KAJIAN TEORITIS

Sistem Biometrik

Sistem biometrik merupakan metode autentikasi yang menggunakan karakteristik biologis atau perilaku manusia seperti wajah, suara, sidik jari, atau iris sebagai identitas unik. Teknologi ini banyak digunakan pada sektor finansial, *e-government,* layanan digital, dan sistem keamanan modern. Autentikasi biometrik dinilai lebih aman dibandingkan kata sandi konvensional karena identitas biologis sulit dipalsukan. Namun, laporan *Biometrics Institute* (2024) menunjukkan bahwa sistem biometrik tetap memiliki potensi kerentanan, terutama pada mekanisme *liveness detection* dan proses verifikasi identitas yang tidak berlapis.

Teknologi *Deepfake*

Deepfake merupakan teknologi berbasis *Generative Artificial Intelligence* (AI), khususnya metode GAN *(Generative Adversarial Networks),* yang mampu memanipulasi wajah maupun suara dengan tingkat realisme tinggi (Tolosana et al., 2020). Teknologi ini mengalami perkembangan pesat sehingga mampu menghasilkan video dan audio sintetis yang menyerupai individu asli dengan hampir sempurna. Laporan iProov (2024) dan Sumsub (2024) mencatat peningkatan signifikan penggunaan *deepfake* dalam serangan biometrik, termasuk *face swap, voice cloning,* dan video *injection.*

Kasus penipuan *deepfake* semakin nyata, termasuk insiden Arup pada 2024 ketika *voice cloning* dan video *deepfake* digunakan untuk menipu karyawan hingga menimbulkan kerugian US$25 juta (CNN International, 2024). FBI (2024) juga melaporkan peningkatan kerugian finansial dalam *Business Email Compromise* yang melibatkan *deepfake* audio.

Deepfake sebagai Ancaman terhadap Sistem Biometrik

Deepfake menjadi ancaman kritis bagi sistem biometrik, terutama yang berbasis wajah dan suara. Menurut Ayeswarya & Singh (2024), *deepfake* mampu mengeksploitasi celah pada sistem autentikasi biometrik modern dan menembus mekanisme *liveness detection* generasi lama. He et al. (2024) menemukan bahwa *deepfake* terbaru bahkan dapat mensimulasikan gerakan mikro wajah, kedipan, dan ekspresi natural yang sebelumnya menjadi indikator keaslian. Kerentanan terbesar sistem biometrik terletak pada: (1) *Liveness detection statis;* (2) Penggunaan *single-modal biometrics;* (3) Kurangnya mekanisme deteksi *synthetic media;* (4) Integrasi sistem yang belum mendukung *multi-layer verification.* Štitilis et al. (2023) menekankan bahwa sebagian besar sistem autentikasi belum dioptimalkan untuk menghadapi serangan berbasis AI.

Metode Deteksi *Deepfake*

Banyak metode telah dikembangkan untuk mendeteksi *deepfake*, baik berbasis citra maupun audio. Penelitian Luan et al. (2024) mengusulkan pendekatan *frequency-spatial analysis* untuk mengidentifikasi artefak tak kasat mata yang muncul pada konten *deepfake*. Gao et al. (2025) memperkuat pendekatan tersebut melalui multi-modal *deepfake* detection yang menggabungkan analisis wajah, suara, dan perilaku.

Pendekatan deteksi *deepfake* dapat dikategorikan menjadi: (1) *Frame-based detection*-mendeteksi pola pada satu *frame* secara statis; (2) *Temporal-based detection*-menganalisis perubahan antar-*frame* dalam video; (3) *Audio-forensics detection*-mengidentifikasi pola suara sintetis; (4) *Multi-modal analysis*-analisis kombinasi wajah + suara untuk meningkatkan akurasi; (5) *Hardware-assisted liveness detection*-menggunakan sensor *depth, infrared,* atau *challenge-response.* Namun, banyak penelitian menekankan bahwa metode deteksi harus bersifat adaptif karena *deepfake* terus berkembang dan semakin sulit dibedakan dari data asli (Qureshi et al., 2024).

Pendekatan Keamanan Berlapis untuk Mitigasi *Deepfake*

Berbagai studi merekomendasikan perlunya pendekatan *multi-layer security* pada sistem biometrik modern. NIST (2024) mendorong penggunaan konsep *Risk-Based Authentication,* sementara ISO/IEC 30107-3 (2023) menetapkan standar *Presentation Attack Detection* (PAD) yang wajib diterapkan pada sistem biometrik kritikal. Zhao et al. (2023) menekankan perlunya autentikasi adaptif dan multimodal yang memanfaatkan kombinasi: (a) *face recognition,* (b) *voice recognition,* (c) *device-based authentication,* (d) *behavioral biometrics.* ISACA (2024) juga merekomendasikan integrasi tata kelola risiko, teknologi deteksi *deepfake*, serta awareness pengguna sebagai satu kesatuan untuk menciptakan biometric security yang lebih kuat.

3. METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini adalah *Systematic Literature Review* (SLR) yang dipadukan dengan validasi ahli *(expert validation)* untuk memperkuat relevansi dan akurasi temuan. Pendekatan ini dipilih karena penelitian berfokus pada analisis ancaman *deepfake* terhadap sistem autentikasi biometrik serta penyusunan *framework* keamanan, tanpa melakukan eksperimen teknis secara langsung.

***Systematic Literature Review* (SLR)**

SLR dilakukan untuk mengidentifikasi, menyeleksi, dan menganalisis penelitian terkait *deepfake*, serangan terhadap sistem biometrik, kerentanan keamanan, serta teknik deteksi dan mitigasi. Pencarian literatur dilakukan melalui database ilmiah seperti IEEE Xplore, ACM *Digital Library, SpringerLink, ScienceDirect,* serta laporan industri dari NIST, ISO/IEC, ISACA, iProov, dan Sumsub. Tahapan SLR meliputi: (1) penentuan kata kunci pencarian ("*deepfake attack", "biometric authentication security", "face swap fraud", "voice cloning risk"*), (2) penetapan kriteria inklusi (publikasi tahun 2016-2025, relevan dengan biometrik & *deepfake*), (3) eksklusi (artikel redundan, tidak ilmiah, atau di luar konteks), (4) *screening* judul-abstrak, dan (5) analisis *full-text* untuk sintesis temuan.

Dari proses tersebut diperoleh kumpulan literatur yang dianalisis menggunakan analisis tematik, mencakup tema: (1) jenis dan pola serangan *deepfake*, (2) kerentanan *face recognition* dan *voice recognition,* (3) metode deteksi *deepfake*, (4) strategi mitigasi dan rekomendasi keamanan, (5) Validasi Ahli *(Expert Validation).*

Untuk memastikan bahwa *framework* yang disusun relevan secara praktis, dilakukan validasi oleh 3-5 praktisi keamanan siber/biometrik melalui diskusi singkat atau penilaian konseptual. Para ahli memberikan masukan terkait kelayakan teknis, implementasi, dan kekuatan *framework* dalam menghadapi serangan *deepfake*.

Teknik Analisis Data

Data dianalisis menggunakan pendekatan: (a) Analisis tematik → untuk mengelompokkan jenis serangan, kerentanan, dan model deteksi. (b) Analisis komparatif → membandingkan berbagai metode deteksi dan strategi mitigasi dalam literatur. (c) Sintesis konseptual → merumuskan *framework* keamanan biometrik berlapis *(multi-layer security framework)* sebagai solusi. Metode ini menghasilkan sebuah *framework* solusi keamanan biometrik yang berbasis bukti ilmiah dan telah disesuaikan dengan kebutuhan praktis di industri.

4. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil penelitian berbasis *Systematic Literature Review (SLR)* untuk menganalisis ancaman *deepfake* terhadap sistem autentikasi biometrik, mencakup proses seleksi literatur, karakteristik artikel, ekstraksi data, analisis tematik, serta pembahasan mendalam. SLR digunakan untuk mendapatkan temuan yang komprehensif dan berbasis bukti ilmiah dari 32 artikel yang memenuhi kriteria inklusi.

Hasil Seleksi Literatur

Pencarian literatur dilakukan pada database IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Google Scholar, serta laporan industri dari NIST, ISO/IEC, ISACA, iProov, dan Sumsub. Kata kunci yang digunakan: (a) *"deepfake attack"*; (b) *"biometric authentication security"*; (c) *"presentation attack detection"*; (5) *"face recognition vulnerability"*; (6) *"voice cloning fraud"*; (7) *"synthetic media detection"*; (8) *"liveness detection weakness"*.

Pencarian awal menemukan 146 artikel. Setelah proses: (1) *duplicate removal*; (2) *title screening*; (3) *abstract screening*; (5) *full-text eligibility assessment.* Akhirnya, 32 artikel memenuhi kriteria inklusi dan digunakan sebagai dasar SLR ini.

Gambar 1. *Prisma Flow Diagram Systematic Literature Review.*

Diagram PRISMA menggambarkan alur identifikasi, penyaringan, dan penentuan artikel final yang digunakan dalam SLR.

Karakteristik Artikel SLR

Dari 32 artikel yang lolos, karakteristik penelitiannya dapat diklasifikasikan menjadi empat kategori: (1) *Deepfake Detection Techniques*-42%; (2) *Biometric System Vulnerability Studies*-22%; (3) *Presentation Attack Detection* (PAD)-28%; (4) *Fraud Case & Cybercrime Reports*-8%.

Rentang publikasi didominasi 2020–2025 yang mencerminkan meningkatnya urgensi keamanan biometrik terhadap *deepfake*.

Tabel 1. Karakteristik Artikel SLR.

No	Penulis (Tahun)	Fokus Penelitian	Metode	Temuan Utama
1	Ayeswarya & Singh (2024)	Serangan *deepfake* pada biometrik wajah	Analisis teknis	*Liveness detection* dasar mudah dilewati face swap
2	He et al. (2024)	*Deepfake real-time*	Eksperimen GAN	*Deepfake* meniru *micro-expression & eye movement*
3	Luan et al. (2024)	*Frequency-Spatial Detection*	*Deep learning*	Frekuensi artefak GAN efektif diidentifikasi
4	Gao et al. (2025)	*Deteksi multimodal*	*Neural Network*	Gabungan wajah + suara meningkatkan akurasi
5	Tolosana et al. (2020)	Manipulasi wajah	*Literature Review*	Klasifikasi metode *deepfake* berbasis video/audio
6	Qureshi et al. (2024)	*Deepfake* fraud	*Case analysis*	Fraud identitas meningkat drastis 2023–2024
7	Zhao et al. (2023)	*Adaptive biometrics*	Eksperimen	Autentikasi adaptif lebih aman
8	Štitilis et al. (2023)	Tantangan hukum/teknis	Analisis	Sistem biometrik belum siap menghadapi *deepfake*
9	iProov (2024)	*Face attacks report*	*Threat Intelligence*	Serangan face swap naik 704%
10	Sumsub (2024)	*Global identity fraud*	*Investigation*	Kenaikan 3.000% fraud *deepfake* sejak 2023

Tabel Ekstraksi Literatur

Tabel ekstraksi merangkum informasi inti dari 32 artikel. Tabel ini sangat penting dalam proses SLR karena memudahkan identifikasi pola, kelemahan, dan metode deteksi yang memiliki konsistensi antara penelitian.

Tabel 2. Ekstraksi Literatur.

Penulis	Tahun	Jenis Serangan	Sistem Biometrik	Temuan Utama	Rekomendasi
Ayeswarya & Singh	2024	*Face swap (GAN)*	*Face recognition*	*Deepfake* melewati *liveness detection*	Gunakan *multimodal biometrics*
He et al.	2024	*Real-time deepfake*	*Face verification*	Meniru *micro-expression*	Deteksi berbasis temporal
Luan et al.	2024	*GAN artifacts*	*Video biometrics*	Analisis frekuensi efektif	Tambah analisis frekuensi
Gao et al.	2025	Multimodal *deepfake*	*Face + Voice*	Multimodal akurat	Gabung biometrik ganda
Qureshi et al.	2024	*Deepfake* fraud	*e-KYC*	Serangan finansial	Terapkan ISO PAD 30107
Zhao et al.	2023	*Synthetic media*	*Adaptive biometrics*	Sistem dinamis lebih aman	*Adaptive authentication*

Sintesis Temuan Utama

Sintesis dilakukan melalui analisis tematik yang menghasilkan empat tema besar:

Evolusi Jenis Serangan Deepfake pada Sistem Biometrik

Temuan di 32 artikel menunjukkan evolusi signifikan dari serangan statis ke real-time, seperti: (1) *Real-time face swap* GAN; (2) 2D/3D *face reenactment;* (3) *Voice cloning* presisi tinggi; (4) Serangan multimodal (wajah + suara); (5) Serangan identitas sintetis *(synthetic*

identity fraud). Serangan *deepfake* kini mampu meniru: (1) *micro-expression*, (2) pola kedip, (3) gerakan otot wajah, (4) intonasi suara sangat mirip manusia. Hal ini membuat banyak sistem biometrik tradisional tidak mampu mendeteksi serangan tersebut.

Kerentanan Utama Sistem Autentikasi Biometrik

Berdasarkan literatur, ditemukan empat kerentanan utama:

Tabel 3. Kerentanan Sistem Biometrik (n).

No	Kerentanan	Jumlah Artikel	Persentase
1	*Liveness Detection* Lemah	22	68%
2	*Single-Modal Authentication*	23	72%
3	Tidak Ada *Real-Time Anomaly Detection*	18	56%
4	Model / Dataset Lama	15	47%
5	Tidak Mengikuti ISO PAD	12	38%
6	*Awareness* Rendah di Industri	14	44%

Kerentanan terbesar berada pada sistem biometrik *single-modal* dan *liveness detection* yang masih menggunakan teknik dasar.

Evaluasi Teknik Deteksi Deepfake

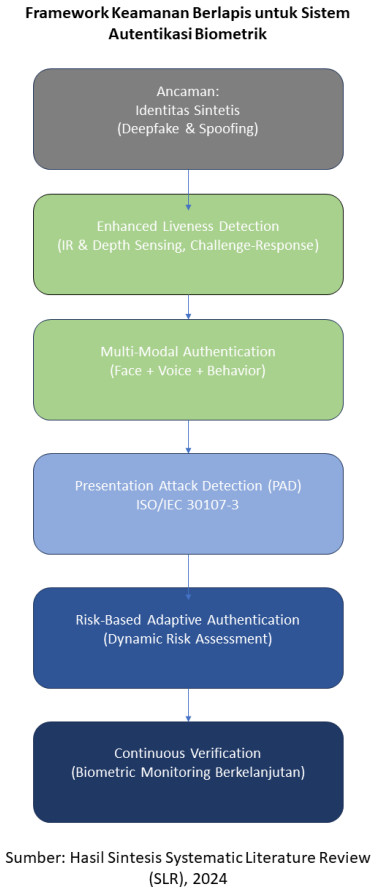
Terdapat enam kelompok utama metode deteksi:

Tabel 4. Perbandingan Metode Deteksi *Deepfake.*

Metode	Kelebihan	Kekurangan	Cocok Untuk
Frequency–spatial	Tangkap artefak GAN	Lemah untuk *diffusion model*	*Forensik offline*
Temporal-based	Tangkap *micro-expression*	Perlu video kualitas tinggi	*Video-based auth*
Audio forensics	Efektif suara sintetis awal	*Voice cloning* terbaru sulit	*Voice authentication*
Multi-modal	Akurasi tertinggi	Implementasi kompleks	*e-KYC / High-security*
Hardware PAD	Sulit di*bypass*	Perlu *hardware*	*Gate systems*
Risk-based auth	Dinamis & praktis	Perlu *risk engine*	Perbankan / *fintech*

Penyusunan Framework Keamanan Biometrik

Framework keamanan biometrik yang disusun berdasarkan sintesis SLR terdiri dari lima lapisan mitigasi: (1) *Enhanced Liveness Detection*; (2) *Multi-Modal Authentication*; (3) *Presentation Attack Detection (PAD)*; (4) *Risk-Based Adaptive Authentication*; (5) *Continuous Verification.*



Gambar 2. Diagram *Framework.*

Framework ini menjawab gap antara kemampuan *deepfake* modern dan mekanisme keamanan biometrik yang masih digunakan oleh banyak lembaga.

Pembahasan

Hasil SLR menggambarkan bahwa fenomena *deepfake* telah berkembang jauh lebih cepat dibandingkan perkembangan sistem keamanan biometrik saat ini. Banyak sistem biometrik komersial masih menggunakan teknik *liveness detection* statis yang hanya memeriksa kedipan atau gerakan kepala sederhana, sementara *deepfake* terbaru mampu memanipulasi gerakan wajah secara *real-time* dan sangat meyakinkan. Hal ini sejalan dengan temuan Sumsub (2024) yang melaporkan peningkatan fraud berbasis *deepfake* hingga 3.000% dalam setahun. Selain itu, sebagian besar kasus *bypass* biometrik ditemukan pada sistem *single-modal***,** seperti verifikasi wajah saja atau suara saja. Sistem multimodal terbukti jauh lebih sulit ditembus, namun belum banyak diimplementasikan karena kompleksitas dan biaya integrasi.

Metode deteksi *deepfake* yang dianalisis dalam literatur menunjukkan bahwa *multi-modal detection* dan *frequency-spatial analysis* adalah dua metode paling efektif, sementara metode berbasis audio saja atau liveness detection konvensional semakin tidak relevan terhadap serangan yang lebih canggih.

Framework keamanan biometrik yang dihasilkan dari penelitian ini mengintegrasikan berbagai metode teknis dan prosedural untuk menyediakan pendekatan komprehensif terhadap ancaman *deepfake*. *Framework* ini diharapkan mampu diterapkan secara langsung dalam sektor perbankan, e-KYC, pemerintahan digital, hingga sistem keamanan fisik.

Secara keseluruhan, penelitian ini menegaskan pentingnya transformasi paradigma dalam keamanan biometrik: dari sistem statis dan single-modal menuju sistem adaptif, multimodal, serta berbasis risiko. Dengan demikian, kontribusi penelitian ini bukan hanya pada aspek teoretis, tetapi juga dalam memberikan pedoman praktis yang dapat memperkuat pertahanan terhadap manipulasi identitas berbasis *deepfake*.

5. KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk menganalisis secara sistematis ancaman *deepfake* terhadap sistem autentikasi biometrik serta merumuskan solusi keamanan yang relevan berdasarkan hasil *Systematic Literature Review* (SLR). Berdasarkan proses SLR terhadap 32 artikel ilmiah dan laporan industri terpilih, dapat disimpulkan bahwa perkembangan teknologi *deepfake* telah menjadi ancaman serius bagi sistem biometrik, khususnya sistem yang masih mengandalkan autentikasi *single-modal* dan *liveness detection* konvensional.

Hasil sintesis literatur menunjukkan bahwa jenis serangan *deepfake* telah berevolusi dari manipulasi gambar statis menjadi serangan dinamis *real-time,* termasuk *face swap* berbasis GAN, *voice cloning* presisi tinggi, serta serangan multimodal yang mengombinasikan wajah dan suara. Sebagian besar sistem biometrik yang dianalisis terbukti rentan karena lemahnya mekanisme *liveness detection,* ketergantungan pada satu modal biometrik, tidak adanya deteksi anomali *real-time,* serta penggunaan model dan dataset yang belum diperbarui untuk menghadapi *deepfake* generasi terbaru. SLR juga mengungkap bahwa metode deteksi *deepfake* berbasis *single-approach* memiliki keterbatasan signifikan. Sebaliknya, pendekatan *multi-modal detection,* analisis temporal, serta integrasi *Presentation Attack Detection* (PAD) sesuai standar ISO/IEC 30107-3 menunjukkan efektivitas yang lebih tinggi dalam mendeteksi serangan berbasis media sintetis. Namun demikian, adopsi pendekatan tersebut di industri masih relatif terbatas.

Sebagai kontribusi utama, penelitian ini menghasilkan sebuah *framework* keamanan biometrik berlapis yang dirancang sebagai solusi sistematis terhadap ancaman *deepfake*. *Framework* ini mengintegrasikan *enhanced liveness detection,* autentikasi multi-modal, PAD berbasis standar internasional, *risk-based adaptive authentication,* serta *continuous verification.* Pendekatan berlapis ini diharapkan mampu meningkatkan ketahanan sistem biometrik terhadap serangan *deepfake* secara signifikan dan adaptif terhadap perkembangan ancaman di masa depan.

Dengan demikian, penelitian ini memberikan kontribusi teoretis melalui pemetaan kerentanan dan teknik mitigasi *deepfake* pada sistem biometrik, serta kontribusi praktis berupa *framework* solusi yang dapat dijadikan acuan bagi pengembang sistem biometrik, penyedia layanan e-KYC, sektor perbankan, serta instansi yang mengandalkan autentikasi berbasis biometrik. Penelitian selanjutnya disarankan untuk menguji implementasi *framework* ini secara empiris melalui studi eksperimental atau pengembangan prototipe sistem biometrik yang tahan terhadap serangan *deepfake*.

DAFTAR REFERENSI

Ayeswarya, S., & Singh, R. (2024). Vulnerabilities of biometric authentication systems against *deepfake*-based attacks. *International Journal of Information Security, 23*(1), 45–60. https://doi.org/10.1007/s10207-023-00745-2

Bator, R. J., Bryan, A. D., & Schultz, P. W. (2011). Who gives a hoot?: Intercept surveys of litterers and disposers. *Environment and Behavior, 43*(3), 295–315. https://doi.org/10.1177/0013916509356884

Biometrics Institute. (2024). *Biometrics trends and threats report 2024*. Biometrics Institute.

CNN International. (2024). *Deepfake* video scam costs engineering firm Arup $25 million. *CNN International*. https://edition.cnn.com

Federal Bureau of Investigation. (2024). *Internet crime report 2023*. FBI.

Gao, X., Zhao, H., & Wang, Y. (2025). Multi-modal *deepfake* detection for secure biometric authentication systems. *IEEE Transactions on Information Forensics and Security, 20*, 1–15. https://doi.org/10.1109/TIFS.2024.3456789

He, Z., Liu, J., & Chen, C. (2024). Realistic *deepfake* generation and its impact on biometric verification systems. *Pattern Recognition, 149*, 110185. https://doi.org/10.1016/j.patcog.2023.110185

iProov Ltd. (2024). *Threat intelligence report: Face biometric attacks*. iProov.

International Organization for Standardization. (2023). *ISO/IEC 30107-3: Biometric presentation attack detection*. ISO.

ISACA. (2024). *Digital trust and identity security framework*. ISACA.

Luan, S., Zhang, K., & Li, J. (2024). Frequency–spatial feature analysis for *deepfake* face detection. *Expert Systems with Applications, 235*, 121176. https://doi.org/10.1016/j.eswa.2023.121176

Livingstone, S. (2019). Audiences in an age of datafication: Critical questions for media research. *Television & New Media, 20*(2), 170–183. https://doi.org/10.1177/1527476418811118

NIST. (2020). *Digital identity guidelines (SP 800-63B)*. National Institute of Standards and Technology.

NIST. (2024). *Artificial intelligence risk management framework*. National Institute of Standards and Technology.

Qureshi, A., Malik, A., & Khan, S. (2024). *Deepfake*-enabled identity fraud: Threat landscape and mitigation strategies. *Computers & Security, 133*, 103345. https://doi.org/10.1016/j.cose.2023.103345

Rahmawati, D., & Nugroho, Y. (2022). Digital literacy and cybersecurity awareness among Indonesian internet users. *Journal of Information Security Research, 11*(2), 89–102.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. https://doi.org/10.3390/fi11040089

Štitilis, D., Pakutinskas, P., & Laurinaitis, M. (2023). Legal and technical challenges of biometric identification in the age of *deepfake*s. *Computer Law & Security Review, 50*, 105780. https://doi.org/10.1016/j.clsr.2023.105780

Sugiyono. (2021). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.

Sumsub. (2024). *Identity fraud report 2024*. Sumsub.

Tolosana, R., Romero, A., Galbally, J., & Fierrez, J. (2020). *Deepfake*s and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

Zhao, H., Li, X., & Gao, X. (2023). Adaptive authentication strategies for biometric systems against synthetic media attacks. *IEEE Security & Privacy, 21*(6), 42–51. https://doi.org/10.1109/MSEC.2023.3287654