Peran Watermark Citra sebagai Lapisan Identitas Biometrik Persisten untuk Arsitektur Tata Kelola dan Interoperabilitas Data Wajah: Kerangka Konseptual pada Ekosistem Aplikasi Digital Terintegrasi

Muhammad Romadhona Kusuma[1], Sepdiyanto[2], Noor Azis[3], Muhammad Sholeh[4]

[1,] *Program Studi Doktor Informatika, Universitas Nusa Mandiri, Indonesia*

[2.] *Fakultas Ilmu Komputer, Universitas Indonesia*

[3.] *Divisi Microfinance, Badan Amil Zakat Indonesia*

[1]*m.romadhona.kusuma@gmail.com,* [2]*sepdiyanto@ui.ac.id,* [3]*noor.azis@baznas.go.id,* [4]*muhammad.sholeh@baznas.go.id*

Intisari— **Pemanfaatan citra wajah sebagai identitas biometrik dalam sistem digital terintegrasi terus meningkat dan menuntut mekanisme pengamanan yang tidak hanya bergantung pada metadata maupun basis data aplikasi. Metadata bersifat tidak persisten dan rentan terhadap penghapusan atau modifikasi, sementara basis data dapat mengalami kehilangan atau ketidaktersediaan dalam jangka panjang. Artikel ini mengusulkan kerangka konseptual watermark citra sebagai lapisan identitas biometrik persisten yang tertanam langsung pada sinyal citra wajah. Arsitektur yang diusulkan terdiri dari Application Layer, Image Processing & Watermark Layer, Storage Layer, serta Verification & Audit Layer. Pendekatan ini dirancang untuk menjaga integritas identitas biometrik, mendukung audit, serta memungkinkan interoperabilitas lintas sistem. Sebagai ilustrasi penerapan, kerangka ini diusulkan pada ekosistem aplikasi Menara Masjid dan Microfinance Masjid yang menggunakan citra wajah sebagai identitas digital pengguna. Hasil perancangan menunjukkan bahwa watermark citra dapat berfungsi sebagai identitas internal yang independen terhadap metadata dan basis data, sekaligus memperkuat tata kelola biometrik dan mendukung pelacakan serta mitigasi penyalahgunaan citra wajah dalam ekosistem aplikasi digital terintegrasi.**

Kata kunci— Watermark Citra, Identitas Biometrik Persisten, Tata Kelola Data, Interoperabilitas, Keamanan Biometrik.

Abstract— **The utilization of facial images as biometric identity in integrated digital systems continues to increase and requires security mechanisms that do not solely depend on metadata or application databases. Metadata is non-persistent and vulnerable to deletion or modification, while databases may experience loss or long-term unavailability. This paper proposes a conceptual framework in which image watermarking functions as a persistent biometric identity layer embedded directly within the facial image signal. The proposed architecture consists of the Application Layer, Image Processing & Watermark Layer, Storage Layer, and Verification & Audit Layer. This approach is designed to preserve biometric identity integrity, support auditing, and enable cross-system interoperability. As an implementation illustration, the framework is proposed for the Menara Masjid and Microfinance Masjid application ecosystem, which utilizes facial images as users' digital identity. The design results indicate that image watermarking can serve as an internal identity independent of metadata and databases, while strengthening biometric governance and supporting traceability as well as mitigation of facial image misuse within an integrated digital application ecosystem.**

Keywords— Image Watermarking, Persistent Biometric Identity, Data Governance, Interoperability, Biometric Security.

I. PENDAHULUAN

Pemanfaatan citra wajah sebagai identitas biometrik dalam sistem digital terus meningkat, khususnya pada sistem layanan terintegrasi yang membutuhkan keandalan identitas jangka panjang dalam berbagai proses bisnis seperti registrasi, autentikasi, dan audit [4]. Identitas berbasis wajah banyak digunakan pada layanan publik, keuangan, dan komunitas, termasuk ekosistem aplikasi yang mendukung pengelolaan masjid dan program keuangan mikro berbasis masjid. Pada konteks pengelolaan masjid, studi evaluatif terhadap Aplikasi Menara Masjid BAZNAS menunjukkan bahwa transformasi digital dapat meningkatkan efektivitas administrasi, transparansi pelaporan, dan kepatuhan terhadap regulasi nasional, namun masih menyisakan ruang penguatan pada aspek keamanan data dan tata kelola identitas [27].

Hal ini membuka kebutuhan untuk merancang lapisan perlindungan yang tidak hanya berfokus pada data tekstual dan transaksi, tetapi juga pada citra wajah sebagai identitas digital yang semakin sering digunakan. Pada praktik umum, identitas citra dalam sistem-sistem tersebut masih bergantung pada: metadata file (misalnya EXIF, properti file, dan tag internal); basis data aplikasi, yang memetakan citra ke entitas pengguna; serta sistem backend, yang mengatur otentikasi, otorisasi, dan integrasi.

Pendekatan ini memiliki keterbatasan mendasar. Metadata dapat hilang atau terhapus ketika citra dikompresi, diproses ulang, diunggah ke platform lain, atau dimigrasikan antar sistem. Basis data dapat mengalami kehilangan data, inkonsistensi, serangan siber, atau ketidaktersediaan ketika sistem dihentikan atau diganti. Dengan demikian, identitas citra tidak bersifat persisten pada level sinyal citra, melainkan bergantung pada struktur eksternal yang rapuh terhadap perubahan.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

Di sisi lain, berbagai kajian menegaskan bahwa data biometrik, termasuk citra wajah, merupakan aset yang sangat sensitif karena sifatnya yang permanen dan tidak dapat "diganti" seperti kata sandi [4], [5]. Kebocoran atau penyalahgunaan citra wajah tidak hanya menimbulkan masalah privasi, tetapi juga berpotensi dimanfaatkan untuk serangan pemalsuan, spoofing, hingga deepfake [6]–[8].
Kebutuhan akan identitas biometrik yang persisten muncul setidaknya dalam empat dimensi utama:

1. Integritas data: memastikan bahwa citra wajah yang digunakan benar-benar berasal dari sumber yang sah dan tidak dimodifikasi secara tak berwenang [8], [16].
2. Audit jangka panjang: menyediakan jejak historis yang dapat ditelusuri kembali ketika terjadi sengketa atau investigasi forensik biometrik.
3. Interoperabilitas lintas sistem: menjaga konsistensi identitas meskipun aplikasi, infrastruktur backend, atau sistem database mengalami perubahan [5], [9].
4. Mitigasi penyalahgunaan dan manipulasi, termasuk indikasi terhadap deepfake dalam konteks verifikasi internal sistem [6]–[8], [19].

Dalam konteks ini, artikel ini mengusulkan watermark citra sebagai lapisan identitas biometrik persisten yang tertanam langsung pada sinyal citra wajah, di mana watermark tidak hanya diposisikan sebagai mekanisme perlindungan hak cipta multimedia [1]–[3], tetapi sebagai identitas internal terproteksi yang melekat pada citra wajah bahkan ketika metadata hilang, dapat diekstraksi dan diverifikasi lintas sistem, mendukung tata kelola, audit, dan pelacakan asal-usul citra, serta membantu mendeteksi manipulasi berat termasuk indikasi deepfake dalam ekosistem aplikasi yang sama, dan sebagai studi konteks kerangka ini diilustrasikan pada ekosistem Aplikasi Menara Masjid dan Aplikasi Microfinance Masjid yang menggunakan citra wajah sebagai bagian dari identitas digital pengurus dan peserta layanan [27].

Tujuan Perancangan kerangka watermark citra sebagai lapisan identitas biometrik persisten memiliki tujuan utama berikut:

1. Mewujudkan persistensi identitas biometrik yang tertanam langsung pada citra wajah sehingga identitas tidak sepenuhnya bergantung pada metadata maupun basis data aplikasi.
2. Menjaga integritas data biometrik terhadap perubahan atau manipulasi citra, baik yang disengaja maupun tidak disengaja.
3. Mendukung tata kelola data dan mekanisme audit identitas jangka panjang, termasuk pelacakan riwayat perekaman dan verifikasi citra biometrik.
4. Memungkinkan interoperabilitas identitas biometrik lintas sistem aplikasi, sehingga citra yang sama tetap dapat diverifikasi meskipun platform atau infrastruktur berganti.
5. Menyediakan lapisan tambahan untuk pelacakan dan proteksi citra wajah, termasuk indikasi terhadap penyalahgunaan identitas atau manipulasi berat (misalnya deepfake) dalam konteks operasional sistem.

II. STUDI PUSTAKA

Bagian ini memaparkan kajian literatur yang relevan sebagai dasar teoritis penelitian dan untuk mengidentifikasi posisi serta celah penelitian yang menjadi landasan pengusulan kerangka yang dikembangkan.

A. Watermark Citra dan Perlindungan Konten

Watermark digital telah lama dikembangkan sebagai mekanisme untuk perlindungan hak cipta, autentikasi konten, dan pelacakan distribusi media digital. Cox et al. [1] mendefinisikan watermarking sebagai penyisipan informasi tersembunyi dalam sinyal media yang tahan terhadap berbagai operasi pemrosesan. Barni dan Bartolini [2] menekankan aspek rekayasa sistem watermarking, meliputi kapasitas, robustness, dan trade-off dengan kualitas visual. Fridrich [3] mengkaji steganografi dan watermarking dari perspektif keamanan informasi pada citra digital.

Penelitian terbaru mengeksplorasi pendekatan berbasis deep learning untuk meningkatkan ketahanan watermark terhadap distorsi dan serangan, serta menyeimbangkan antara kualitas, kapasitas, dan robustness [6]. Di sisi lain, Wang et al. [8] menunjukkan bahwa watermark dapat digunakan sebagai mekanisme verifikasi integritas dan keaslian citra dalam aplikasi autentikasi.

B. Biometrik dan Keamanan Template

Dalam domain biometrik, Jain et al. [4] menekankan pentingnya keandalan dan keamanan sistem pengenalan biometrik, termasuk pengelolaan template dan data biometrik yang tidak dapat diubah seperti password. Kajian lanjutan menyoroti keamanan template biometrik sebagai isu krusial, karena kebocoran template sulit untuk dipulihkan [5].
Galbally et al. [7] mengulas metode anti-spoofing dalam pengenalan wajah, menegaskan risiko serangan berbasis rekaman statis, foto, dan manipulasi video. Standar ISO/IEC 24745 [9] merumuskan prinsip perlindungan informasi biometrik, menekankan aspek keamanan, integritas, dan privasi dalam pengelolaan sistem biometrik.

C. Watermark untuk Keamanan Biometrik

Beberapa penelitian menggabungkan watermark dengan biometrik untuk memperkuat keamanan. Khan dan Zhang [19] menunjukkan bahwa watermark dapat digunakan untuk mengamankan template biometrik dengan menyisipkan informasi verifikasi ke dalam citra biometrik itu sendiri. Caldelli et al. [20] mengkaji reversible watermarking untuk kebutuhan autentikasi dan pemulihan citra asli.

Di Indonesia, Munir [11], Sutoyo et al. [12], Kadir dan Susanto [13], serta Prasetyo [14] memberikan dasar teoritis mengenai pengolahan citra dan teknik transformasi yang relevan dengan implementasi watermarking. Munir [15] mengulas steganografi dan watermarking pada citra digital, sementara Hidayat dan Harjoko [16] menerapkan watermarking berbasis DWT untuk pengamanan citra. Kusumadewi [17] membahas keamanan biometrik dalam sistem identifikasi digital, dan Setiawan serta Hidayat [18]

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

mengeksplorasi implementasi watermarking untuk perlindungan integritas citra digital.

D. Transformasi Digital Pengelolaan Masjid

Pada konteks manajemen masjid, Kusuma [27] melakukan studi evaluatif terhadap Aplikasi Menara Masjid BAZNAS, yang menyoroti transformasi digital pengelolaan masjid berbasis inovasi sistem informasi dan regulasi nasional. Penelitian tersebut menunjukkan bahwa pemanfaatan aplikasi digital dapat meningkatkan transparansi administrasi, pelaporan ZIS, dan keselarasan dengan regulasi nasional. Namun, aspek keamanan biometrik dan pengelolaan identitas wajah belum menjadi fokus utama.

Artikel ini melengkapi kajian tersebut dengan mengusulkan kerangka watermark citra sebagai lapisan identitas biometrik persisten yang dapat diintegrasikan ke dalam ekosistem aplikasi yang sama, yakni Menara Masjid dan Microfinance Masjid, sehingga dimensi tata kelola identitas biometrik dan keamanan citra wajah memperoleh landasan konseptual yang lebih kuat.

D. . Kontribusi Ilmiah

Berbeda dengan pendekatan watermark tradisional yang umumnya difokuskan pada perlindungan hak cipta, autentikasi konten, dan pelacakan distribusi media digital, penelitian ini memposisikan watermark sebagai lapisan identitas biometrik persisten yang tertanam langsung pada sinyal citra wajah. Dalam kerangka ini, watermark tidak hanya berfungsi sebagai mekanisme proteksi konten, tetapi sebagai identitas internal yang mendukung tata kelola, audit, interoperabilitas, serta verifikasi integritas biometrik lintas sistem.

TABEL I. PERBANDINGAN POSITIONING WATERMARK TRADISIONAL DAN WATERMARK BIOMETRIK PERSISTEN

Aspek	Watermark Tradisional	Watermark Biometrik Persisten (Penelitian Ini)
Tujuan	Perlindungan hak cipta dan autentikasi media	Identitas biometrik persisten
Cakupan	Media digital	Sistem identitas biometrik
Payload	Arbitrary / informasi umum	Payload identitas (Hash(UserID), SystemID, Signature, Timestamp)
Peran	Proteksi konten	Tata kelola identitas dan audit
Ketergantungan	Metadata / file system	Melekat pada sinyal citra
Interoperabilitas	Terbatas	Lintas aplikasi dan sistem
Fungsi keamanan	Proteksi konten	Integritas, tracking, dan mitigasi manipulasi

Kontribusi utama penelitian ini dapat dirangkum sebagai berikut:

1. Positioning baru watermark citra sebagai lapisan identitas biometrik persisten yang tertanam langsung pada sinyal citra wajah, melampaui peran tradisionalnya sebagai pelindung hak cipta [1]–[3].
2. Penyediaan lapisan identitas yang independen dari metadata dan basis data, sehingga identitas tetap dapat diverifikasi meskipun terjadi penghapusan metadata, migrasi sistem, atau gangguan pada basis data.
3. Perancangan kerangka tata kelola dan audit biometrik berbasis watermark, dengan penekanan pada integritas, pelacakan temporal, dan jejak audit historis [9], [16]–[18].
4. Penguatan interoperabilitas identitas lintas aplikasi digital, khususnya pada ekosistem Menara Masjid–Microfinance Masjid, melalui penggunaan payload watermark sebagai lapisan identitas bersama (shared identity layer) [5], [9], [27].
5. Penyediaan dasar konseptual pengembangan plugin keamanan biometrik lintas sistem, yang dapat diintegrasikan ke berbagai aplikasi tanpa perlu merombak arsitektur inti, selama aplikasi tersebut dapat mengakses modul embed–extract dan manajemen kunci.
6. Penajaman peran watermark sebagai lapisan pelacakan dan mitigasi penyalahgunaan citra wajah, dengan memanfaatkan payload sebagai jejak identitas (provenance) untuk mendukung penelusuran sumber citra, memperkuat klaim keaslian (copyright-like provenance dalam konteks biometrik), serta membantu deteksi manipulasi berat termasuk potensi serangan deepfake dalam skenario verifikasi biometrik internal [6]–[8], [19], [20].

III. METODOLOGI PENELITIAN

Berdasarkan tujuan dan kerangka konseptual penelitian yang telah diuraikan pada bagian sebelumnya, bagian ini menjelaskan data, tahapan dan alur penelitian, pendekatan.

1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan rekayasa konseptual berbasis design science, di mana fokus utama bukan pada eksperimen numerik, tetapi pada:

a. Perumusan masalah dan kebutuhan sistem identitas biometrik persisten;
b. Perancangan artefak berupa model arsitektur dan mekanisme watermark biometrik;
c. Justifikasi konseptual melalui analisis literatur, pemodelan arsitektur, dan pemetaan ke skenario implementasi di ekosistem aplikasi nyata.

Artefak yang dikembangkan adalah model arsitektur empat lapisan untuk pengelolaan identitas biometrik persisten berbasis watermark, mekanisme payload dan embedding watermark sebagai identitas internal, model operasional penyimpanan dan verifikasi, serta rancangan integrasi pada ekosistem Menara Masjid dan Microfinance Masjid..

2. Tahapan Penelitian

Tahapan penelitian dirancang secara sistematis untuk membangun kerangka identitas biometrik persisten berbasis watermark, mulai dari kajian teoritis hingga pemetaan implementasi, guna memastikan kerangka yang diusulkan

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

memiliki dasar konseptual, struktural, dan operasional yang jelas, dengan tahapan penelitian meliputi:

a. Studi Literatur
   Mengkaji literatur tentang watermarking [1]–[3], [6], [8], keamanan biometrik [4], [5], [7], [19], perlindungan informasi biometrik [9], pengolahan citra digital [11]–[14], serta pedoman dan regulasi keamanan informasi dan data pribadi [21]–[26].
b. Analisis Kebutuhan dan Celah (Gap Analysis)
   Menganalisis kelemahan pendekatan penyimpanan identitas berbasis metadata dan basis data murni, terutama dari sisi persistensi identitas, interoperabilitas, auditabilitas, pelacakan, dan mitigasi manipulasi citra.
c. Perancangan Kerangka Konseptual
   Menyusun kerangka arsitektur identitas biometrik berbasis watermark dengan pembagian ke dalam Application Layer, Image Processing & Watermark Layer, Storage Layer, serta Verification & Audit Layer.
d. Perancangan Mekanisme Payload dan Embedding
   Merancang struktur payload watermark (Hash(UserID), SystemID, IntegritySignature, Timestamp opsional), serta mekanisme encoding dan penyisipan ke dalam citra wajah, dengan mengacu pada prinsip keamanan template biometrik dan pengolahan citra [5], [11]–[14], [16]–[18].
e. Perumusan Model Operasional dan Roadmap Implementasi
   Menyusun alur operasional (penyimpanan dan verifikasi) serta roadmap implementasi bertahap, mulai dari desain konseptual, prototipe, hingga deployment pilot.
f. Pemetaan ke Studi Kasus Menara Masjid dan Microfinance Masjid
   Mengintegrasikan kerangka yang diusulkan dengan proses bisnis dan alur data pada dua aplikasi tersebut sebagai contoh penerapan di ekosistem layanan keummatan [27].

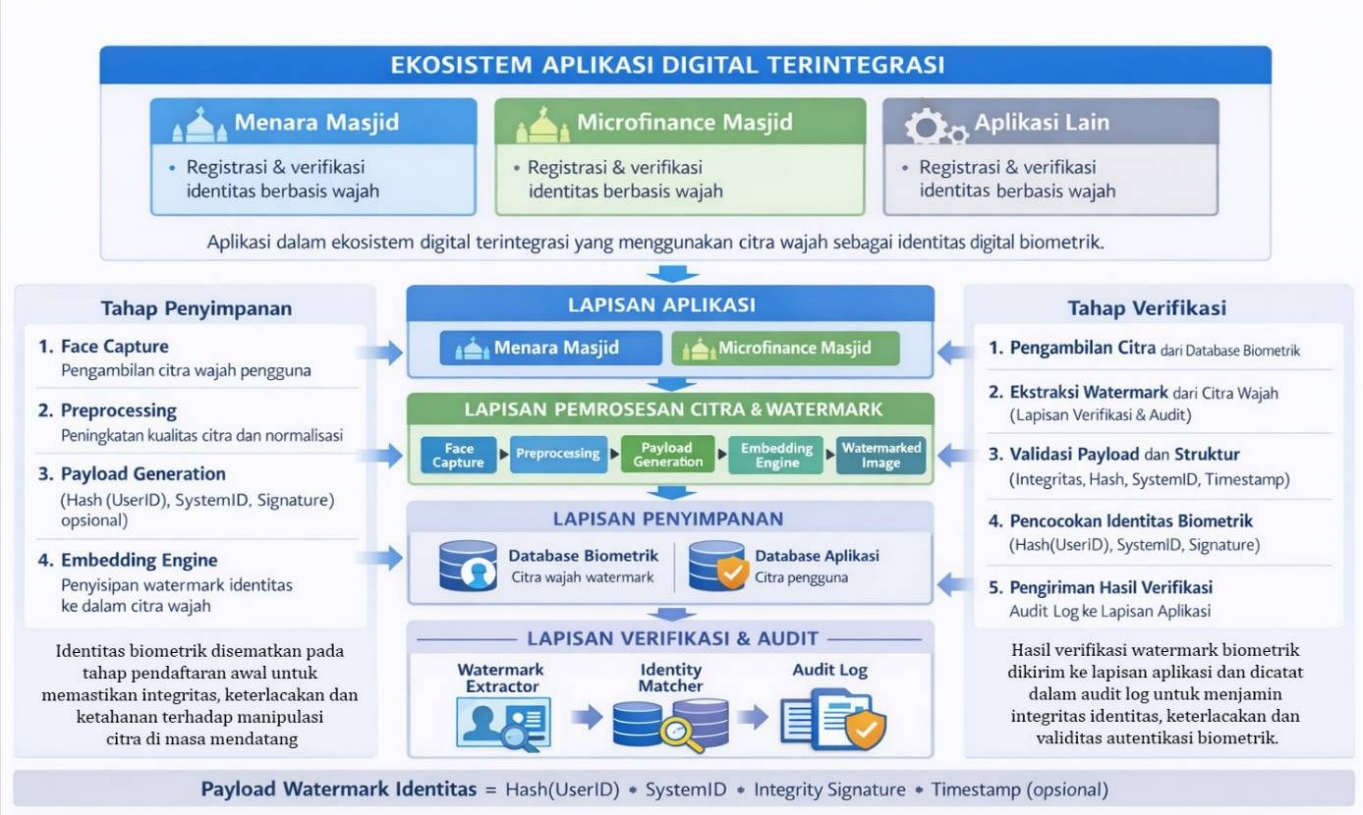
Meskipun artikel ini bersifat konseptual, kerangka evaluasi disiapkan sebagai dasar penelitian lanjutan, antara lain metrik kualitas citra: PSNR, SSIM, dan metrik visual lain untuk menilai dampak embedding terhadap kualitas citra [6], [8], [11]–[14], metrik keberhasilan watermark: Bit Error Rate (BER), tingkat keberhasilan ekstraksi payload, dan robustness terhadap distorsi (kompresi JPEG, noise, cropping, rescaling), metrik interoperabilitas: tingkat keberhasilan verifikasi payload lintas aplikasi (misalnya Menara Masjid ↔ Microfinance Masjid), serta metrik keamanan: kemampuan sistem mendeteksi kegagalan ekstraksi atau ketidaksesuaian payload pada citra yang dimanipulasi atau berpotensi deepfake [6]–[8], [19].

IV. Hasil dan Pembahasan

Berdasarkan perumusan konseptual yang telah diuraikan pada bagian sebelumnya, penelitian ini mengusulkan suatu arsitektur kerangka identitas biometrik berbasis watermark sebagai pendekatan untuk memperkuat pengelolaan identitas digital yang lebih andal, persisten, dan terintegrasi. Kerangka yang diusulkan berfokus pada penanaman identitas biometrik langsung pada sinyal citra wajah sehingga identitas tidak semata bergantung pada metadata maupun basis data eksternal.

Arsitektur tersebut dirancang dalam empat lapisan utama yang saling terhubung dan membentuk siklus pengelolaan identitas biometrik persisten, mulai dari proses akuisisi dan penyisipan watermark, penyimpanan citra yang telah mengandung identitas internal, hingga tahap verifikasi dan audit lintas sistem. Melalui struktur berlapis ini, kerangka diharapkan mampu mendukung integritas identitas biometrik, interoperabilitas antar aplikasi, serta mekanisme pelacakan dan verifikasi jangka panjang dalam ekosistem sistem digital terintegrasi

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267



Gambar 1. Arsitektur Watermark Citra sebagai Lapisan Identitas Biometrik Persisten dalam Ekosistem Aplikasi Digital Terintegrasi

A. Application Layer

Lapisan ini mencakup aplikasi yang memanfaatkan identitas biometrik wajah sebagai bagian dari mekanisme identifikasi dan pengelolaan layanan digital dalam ekosistem terintegrasi:

1. Aplikasi Menara Masjid
   Platform informasi dan manajemen masjid yang mengintegrasikan profil masjid, data pengurus, laporan kegiatan, serta pelaporan ZIS secara digital [27]. Citra wajah digunakan sebagai identitas visual pengurus dan akun dengan hak akses administratif.
2. Aplikasi Microfinance Masjid
   Platform layanan pembiayaan dan pemberdayaan ekonomi berbasis masjid yang mencakup registrasi dan verifikasi peserta. Citra wajah dimanfaatkan sebagai identitas biometrik untuk mendukung keabsahan data peserta dalam proses layanan.
3. Aplikasi Lain dalam Ekosistem Terintegrasi
   Aplikasi lain yang dapat terhubung di masa depan dan memanfaatkan citra wajah sebagai identitas pengguna, sehingga memerlukan konsistensi dan interoperabilitas lintas sistem.

Application Layer bertanggung jawab atas akuisisi citra wajah (*face capture*), interaksi pengguna, serta pengiriman data biometrik ke lapisan pemrosesan watermark.

B. Image Processing & Watermark Layer

Lapisan ini merupakan inti mekanisme watermark biometrik dengan pipeline:
Face Capture → Preprocessing → Payload Generator → Embedding Engine → Watermarked Image

1. Preprocessing: mencakup cropping wajah, alignment, normalisasi intensitas, dan peningkatan kualitas dasar untuk meningkatkan stabilitas embedding dan ekstraksi [11]–[14].
2. Payload Generator: membentuk payload watermark dari Hash(UserID), SystemID, IntegritySignature, dan Timestamp.
3. Embedding Engine: menyisipkan payload ke dalam citra wajah menggunakan algoritma tertentu (misalnya transform domain berbasis DWT/DCT/SVD, atau pendekatan deep learning [1], [2], [6], [16], [18]).

Watermark disisipkan sebagai invisible watermark sehingga tidak mengganggu tampilan visual citra, namun dapat diekstraksi kembali dengan reliabilitas tinggi.

C. Storage Layer

Lapisan ini mengelola penyimpanan data, terdiri dari:

1. Database biometrik, yang menyimpan citra wajah yang telah mengandung watermark;
2. Database aplikasi, yang menyimpan atribut pengguna, profil usaha, riwayat transaksi, dan informasi lain yang tidak tertanam dalam watermark.

Citra yang disimpan dalam database biometrik adalah citra watermarked, bukan citra mentah. Hal ini memastikan bahwa identitas biometrik melekat langsung pada citra, sementara basis data dan metadata berperan sebagai lapisan referensi tambahan.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

D. Verification & Audit Layer

Lapisan ini bertanggung jawab untuk:

- Ekstraksi watermark dari citra wajah yang akan diverifikasi;
- Validasi payload identitas, termasuk pemeriksaan integritas dan keabsahan;
- Pencocokan identitas lintas sistem, misalnya antara entitas pengguna di Menara Masjid dan Microfinance Masjid;
- Pencatatan audit log, yang merekam setiap aktivitas verifikasi, kegagalan ekstraksi, maupun indikasi manipulasi [9], [16]–[18].

Verification & Audit Layer menjadi fondasi tata kelola identitas biometrik jangka panjang karena menyediakan jejak verifikasi dan perubahan yang dapat diaudit.

E. Mekanisme Watermark Biometrik

1. Payload Identitas

Payload watermark dirancang dengan struktur:

Payload = Hash(UserID) || SystemID || IntegritySignature || Timestamp (opsional)

a. Hash(UserID) mengabstraksi identitas pengguna sehingga tidak tersimpan dalam bentuk plaintext.
b. SystemID menandakan asal sistem (misalnya "MENARA" atau "MICROFINANCE"), memungkinkan verifikasi lintas aplikasi.
c. IntegritySignature digunakan untuk mendeteksi perubahan tak sah terhadap payload dan citra.
d. Timestamp (opsional) mendukung pelacakan temporal dan audit historis.

Payload kemudian di-encode menjadi bitstream dan disisipkan ke dalam domain tertentu pada citra (spatial atau transform domain).

2. Watermark sebagai Identitas Persisten

Watermark dapat diklasifikasikan menjadi:

a. Visible watermark (opsional), seperti logo lembaga atau teks kecil, untuk keperluan dokumentasi publik.
b. Invisible watermark (utama), yang tertanam pada sinyal citra tanpa terlihat secara visual.

Invisible watermark inilah yang difungsikan sebagai lapisan identitas biometrik persisten, sehingga citra wajah selalu membawa jejak identitas yang dapat diverifikasi meskipun metadata hilang atau basis data mengalami gangguan.

F. Fungsi Keamanan

Watermark biometrik memberi beberapa fungsi keamanan:

- Verifikasi integritas identitas: memeriksa kecocokan payload dengan entitas pengguna di basis data.
- Deteksi manipulasi citra: kegagalan ekstraksi payload atau ketidaksesuaian IntegritySignature mengindikasikan adanya modifikasi signifikan [8], [16].
- Mitigasi serangan deepfake dalam konteks internal: deepfake atau citra yang dimanipulasi berat cenderung merusak watermark atau menghasilkan payload yang tidak valid [6]–[8], [19].
- Pelacakan asal-usul citra: keberadaan watermark resmi memudahkan penelusuran apakah citra tersebut berasal dari ekosistem aplikasi yang sah atau tidak [19], [20].

Dengan demikian, watermark tidak hanya menjadi identitas, tetapi juga sensor integritas dan instrumen forensik digital.

G. Model Operasional

1. Tahap Penyimpanan (Enrollment)

Alur operasional pada tahap penyimpanan identitas biometrik adalah:

a. Face Capture: sistem menangkap citra wajah pengguna dari kamera atau sumber lain.
b. Preprocessing: citra diproses untuk meningkatkan konsistensi (cropping, alignment, normalisasi).
c. Payload Generation: sistem membentuk payload dari Hash(UserID), SystemID, IntegritySignature, dan Timestamp.
d. Watermark Embedding: bitstream payload disisipkan ke citra menggunakan algoritma watermarking.
e. Storage: citra watermarked disimpan pada database biometrik; data terkait lainnya disimpan di database aplikasi.

Tahap ini memastikan bahwa sejak awal penyimpanan, setiap citra wajah identitas utama telah membawa watermark biometrik persisten.

H. Tahap Verifikasi

Alur operasional pada tahap verifikasi meliputi:

1. Pengambilan citra dari basis data (arsip) atau hasil *capture* baru (misalnya pada proses login biometrik).
2. Ekstraksi watermark dan validasi struktur payload.
3. Pencocokan payload dengan data pengguna di basis data (Hash(UserID), SystemID, IntegritySignature).
4. Analisis hasil:
   a. Jika payload valid dan sesuai → proses verifikasi dapat dilanjutkan dengan pengenalan wajah konvensional;
   b. Jika payload tidak valid atau gagal diekstraksi → sistem dapat menandai citra sebagai "berisiko tinggi" dan meminta verifikasi tambahan (misalnya manual).
5. Pencatatan audit log untuk setiap verifikasi, termasuk keberhasilan atau kegagalan.

I. Roadmap Implementasi

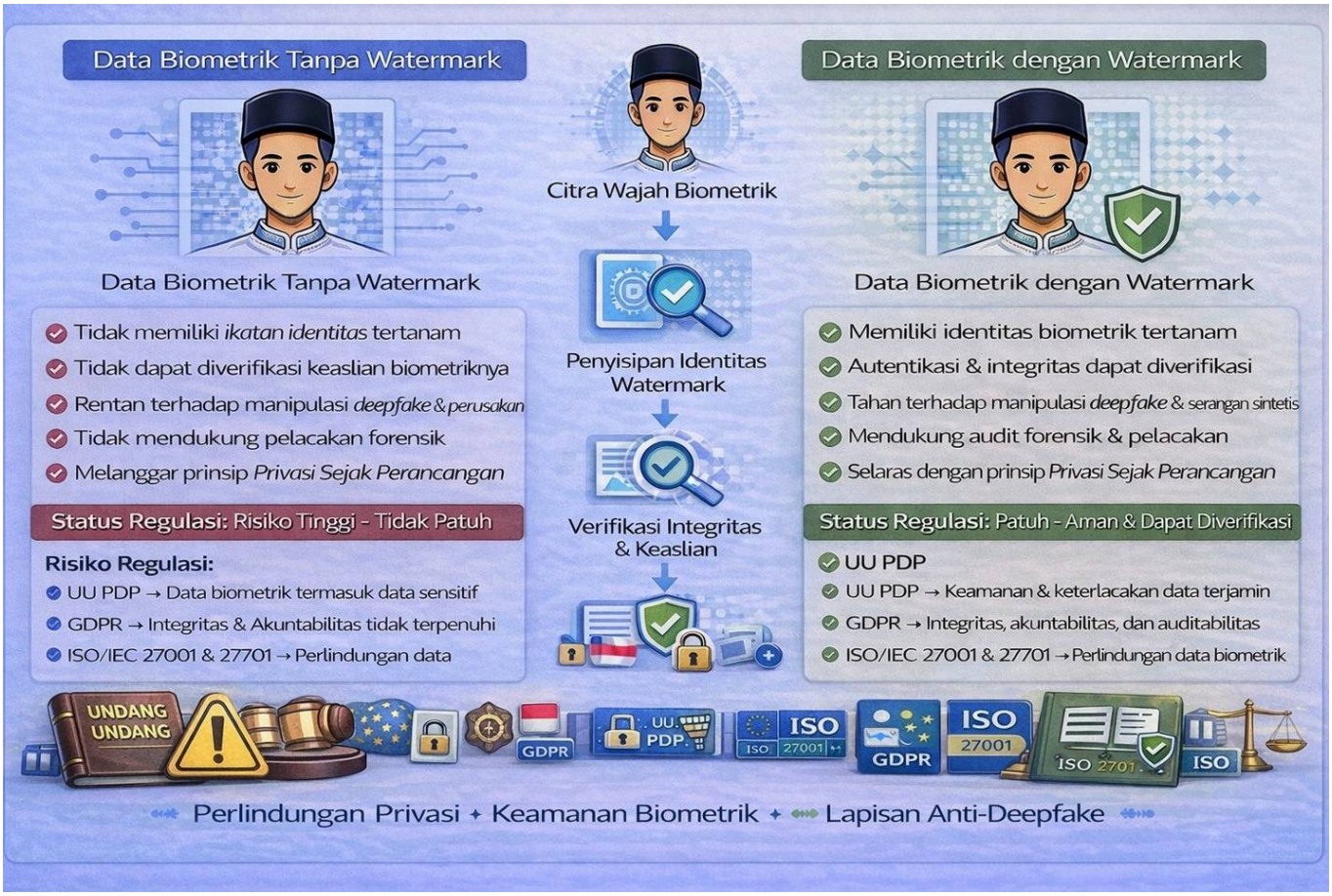
Roadmap implementasi yang diusulkan:

1. Fase 1 – Desain & Simulasi: penyusunan skema payload, pemilihan algoritma embedding, dan pengujian awal pada dataset citra wajah.
2. Fase 2 – Prototipe Embedding–Extraction: pengembangan modul perangkat lunak dan integrasi awal dengan Menara Masjid/Microfinance Masjid pada lingkungan uji.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

3. Fase 3 – Evaluasi Robustness dan Keamanan: pengujian terhadap kompresi, noise, cropping, rescaling, dan skenario manipulasi lainnya, termasuk pengujian terhadap citra yang dimanipulasi (misalnya deepfake sederhana) [6]–[8], [19], [20].
4. Fase 4 – Deployment Pilot: implementasi terbatas di beberapa masjid atau unit layanan microfinance untuk menilai aspek teknis, operasional, dan penerimaan pengguna.

J. Analisis Keamanan dan Tata Kelola



Gambar 2. Perbandingan Data Biometrik Tanpa Watermark dan dengan Watermark sebagai Lapisan Identitas Biometrik Persisten.

Ilustrasi menunjukkan bahwa watermark memungkinkan identitas biometrik tertanam langsung pada sinyal citra, mendukung verifikasi integritas, audit forensik, serta ketahanan terhadap manipulasi termasuk deepfake, sekaligus selaras dengan prinsip perlindungan data dan regulasi biometrik.

1. Threat Model

Ancaman yang relevan untuk sistem biometrik berbasis citra wajah meliputi:

a. Penghapusan atau perubahan metadata;
b. Kehilangan atau kebocoran basis data;
c. Manipulasi citra (editing, filtering, cropping ekstrem);
d. Serangan spoofing berbasis foto/video;
e. Produksi deepfake yang mengganti identitas wajah;
f. Rebinding identitas dengan mengganti entitas di backend tanpa mengubah citra.

Bagian ini menganalisis peran watermark citra sebagai lapisan identitas biometrik persisten dalam menjaga integritas, verifikasi identitas, auditabilitas, interoperabilitas, serta mitigasi manipulasi citra termasuk deepfake, sekaligus kesesuaiannya dengan prinsip keamanan dan regulasi perlindungan data.

2. Peran Watermark dalam Tata Kelola

Dengan menanamkan identitas pada level sinyal citra, watermark menyediakan:

a. Lapisan verifikasi independen dari metadata dan basis data tunggal;
b. Instrumen audit dengan payload yang memuat informasi waktu dan identitas sistem;
c. Penanda keaslian bahwa citra berasal dari ekosistem aplikasi resmi;
d. Landasan forensik digital ketika terjadi sengketa identitas atau dugaan manipulasi [9], [16]–[18].

3. Perbandingan Pendekatan Penyimpanan Identitas Wajah

Untuk memperjelas posisi pendekatan yang diusulkan, Tabel 2 menyajikan perbandingan antara penyimpanan identitas berbasis metadata, basis data, dan watermark pada

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

citra dari sisi persistensi identitas, ketergantungan sistem, interoperabilitas, dukungan audit, serta ketahanan terhadap manipulasi citra.

TABEL II. PERBANDINGAN PENDEKATAN PENYIMPANAN IDENTITAS WAJAH

Pendekatan	Persistensi Identitas	Ketergantungan terhadap Sistem	Interoperabilitas Lintas Aplikasi	Dukungan Audit Jangka Panjang	Ketahanan terhadap Manipulasi Citra
Metadata	Rendah (mudah dihapus/diubah)	Tinggi (terikat pada file system & format)	Rendah (sering hilang saat kompresi/migrasi)	Terbatas (tidak selalu terekam dalam log sistem)	Rendah (tidak merefleksikan perubahan konten citra)
Database	Sedang (tergantung backup & manajemen DB)	Tinggi (bergantung pada infrastruktur backend)	Sedang (membutuhkan integrasi lintas sistem)	Sedang (memerlukan desain logging & audit yang baik)	Terbatas (tidak terkait langsung dengan sinyal citra)
Watermark pada Citra	Tinggi (melekat pada sinyal citra)	Menengah (butuh modul embed–extract, tidak bergantung satu DB)	Tinggi (payload dapat diverifikasi di berbagai aplikasi)	Tinggi (payload dapat memuat timestamp & signature)	Tinggi (kerusakan watermark mengindikasikan manipulasi signifikan)

Tabel ini menegaskan bahwa watermark memberikan keunggulan pada aspek persistensi identitas, interoperabilitas, audit jangka panjang, dan ketahanan terhadap manipulasi citra dibandingkan pendekatan yang hanya mengandalkan metadata dan basis data.

4. Watermark untuk Pelacakan, Kepemilikan, dan Mitigasi Deepfake

Selain sebagai lapisan identitas biometrik persisten, watermark berperan penting dalam pelacakan (tracking) data wajah, proteksi kepemilikan, dan mitigasi manipulasi:

a. Pelacakan asal-usul (provenance) Payload watermark yang berisi Hash(UserID), SystemID, dan IntegritySignature dapat dipandang sebagai bentuk *fingerprint* atau *ownership token* yang melekat pada citra. Jika suatu citra wajah ditemukan di luar sistem (misalnya pada pihak ketiga), keberadaan watermark memungkinkan penelusuran apakah citra tersebut memang berasal dari ekosistem Menara Masjid/Microfinance Masjid atau bukan [19], [20], [27].

b. Peningkatan keamanan saat verifikasi biometrik Pada saat verifikasi berbasis scan wajah, sistem tidak hanya membandingkan fitur wajah, tetapi juga memeriksa payload watermark. Jika payload tidak valid, IntegritySignature gagal, atau Hash(UserID) tidak konsisten dengan identitas yang diklaim, sistem dapat menandai verifikasi sebagai "berisiko" dan membutuhkan langkah tambahan. Dengan demikian, watermark berfungsi sebagai lapisan verifikasi ganda di atas algoritma pengenalan wajah [4], [5], [7], [19].

c. Mitigasi manipulasi citra dan serangan deepfake Watermark tidak dapat mencegah pihak eksternal membuat deepfake di luar sistem, tetapi dapat digunakan untuk mendeteksi dan menolak citra yang tidak sah di dalam ekosistem:

   1. Jika citra tidak mengandung watermark resmi, sementara protokol mewajibkan seluruh citra identitas telah di-watermark, citra tersebut dapat dianggap bukan bagian dari sistem.
   2. Jika citra telah dimanipulasi secara signifikan (misalnya diganti wajahnya dengan deepfake), kemungkinan besar watermark rusak atau payload tidak lagi valid. Kegagalan ekstraksi atau ketidaksesuaian IntegritySignature dapat menjadi indikator kuat adanya manipulasi [6]–[8], [19].

d. Konsistensi dengan tata kelola dan forensik digital Setiap proses ekstraksi dan verifikasi watermark dapat dicatat dalam audit log, menghasilkan jejak forensik yang membantu investigasi ketika terjadi sengketa, dugaan penipuan, atau penyalahgunaan citra biometrik.

Dengan demikian, watermark citra berfungsi tidak hanya sebagai lapisan identitas biometrik persisten, tetapi juga sebagai instrumen pelacakan, proteksi, dan mitigasi risiko deepfake dalam ekosistem aplikasi yang memanfaatkan citra wajah.

K. Aspek Etik, Regulasi, dan Perlindungan Data Biometrik

1. Prinsip Privasi dan Data Pribadi

Kerangka yang diusulkan memanfaatkan payload berupa Hash(UserID) dan SystemID, bukan menyimpan identitas dalam bentuk teks terbuka. Pendekatan ini sejalan dengan prinsip *data minimization* dan *privacy by design*, di mana data yang tertanam dalam watermark dibatasi pada identitas terproteksi yang hanya dapat diinterpretasikan oleh sistem berwenang [5], [9].

Perekaman dan pemrosesan citra biometrik diasumsikan dilakukan dengan persetujuan (consent) dari subjek data, dengan penjelasan yang jelas mengenai tujuan, ruang lingkup pemrosesan, dan hak-hak mereka.

2. Kepatuhan terhadap Regulasi Nasional

Secara nasional, Indonesia telah memiliki kerangka regulasi terkait perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi [24]. Badan Siber dan Sandi Negara (BSSN) mengeluarkan pedoman keamanan informasi dan perlindungan data digital [21], sementara Kementerian

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

Komunikasi dan Informatika merumuskan strategi nasional keamanan siber dan perlindungan data [22]. Kerangka watermark biometrik dapat diselaraskan dengan regulasi tersebut melalui:

a. Pembatasan akses ke modul embed–extract dan manajemen kunci;
b. Pencatatan aktivitas verifikasi sebagai bagian dari *security monitoring*;
c. Penyusunan SOP yang mengatur penggunaan data biometrik, termasuk penonaktifan identitas ketika subjek data mencabut persetujuan sesuai UU PDP [24].

3. Standar Internasional dan ISO

Di tingkat internasional, General Data Protection Regulation (GDPR) mengkategorikan data biometrik sebagai *special category of personal data* yang membutuhkan perlindungan tambahan dan dasar hukum yang kuat [23].
Dari sisi standar:

a. ISO/IEC 27001 menyediakan kerangka *Information Security Management System (ISMS)* untuk pengelolaan keamanan informasi, termasuk aset biometrik [25].
b. ISO/IEC 27701 memperluas ISO/IEC 27001 dengan *Privacy Information Management System (PIMS)*, mengatur tata kelola privasi dan data pribadi [26].

Modul watermark biometrik dapat dimasukkan sebagai bagian dari kontrol teknis dalam ISMS/PIMS, khususnya pada pengelolaan identitas digital, logging, dan verifikasi integritas data.

4. Implikasi Desain Sistem

Beberapa implikasi praktis:

a. Kebutuhan dokumentasi dan DPIA
Sistem yang menggunakan biometrik secara luas sebaiknya dilengkapi dengan *Data Protection Impact Assessment (DPIA)*, untuk mengidentifikasi risiko dan langkah mitigasi.
b. Pengelolaan kunci dan algoritma
Kunci dan parameter algoritma watermark harus diperlakukan sebagai aset kritis, dengan kebijakan rotasi, penyimpanan aman, dan pembatasan akses.
c. Pemisahan peran (segregation of duties)
Peran pengembang, operator, dan auditor sebaiknya dibedakan untuk menjaga independensi proses verifikasi dan audit.
d. Konsistensi dengan hak subjek data
Sistem harus menyediakan mekanisme untuk memenuhi hak akses, koreksi, pembatasan pemrosesan, dan penghapusan data sejauh tidak bertentangan dengan kebutuhan keamanan biometrik dan regulasi yang berlaku [23], [24].

L. Contoh Usulan Implementasi pada Ekosistem Aplikasi

Bagian ini mengilustrasikan penerapan kerangka yang diusulkan pada ekosistem Aplikasi Menara Masjid dan Microfinance Masjid sebagai studi konteks operasional.

1. Konteks Ekosistem Aplikasi Menara Masjid dan Microfinance Masjid

Aplikasi Menara Masjid adalah platform informasi dan manajemen masjid yang mengintegrasikan profil masjid, data pengurus, laporan kegiatan, serta pelaporan ZIS secara digital [27]. Citra wajah digunakan sebagai identitas visual pengurus, pengelola, dan akun tertentu dengan hak akses administratif, sehingga kebutuhan akan tata kelola identitas biometrik yang kuat menjadi relevan.

Aplikasi Microfinance Masjid berfokus pada pengelolaan program pembiayaan dan pemberdayaan ekonomi berbasis masjid, mencakup pendataan peserta, penilaian kelayakan, penyaluran dana, monitoring angsuran, dan pendampingan usaha. Pada konteks ini, citra wajah peserta digunakan sebagai identitas biometrik untuk mendukung proses registrasi, verifikasi identitas, dan dokumentasi interaksi layanan.

Kedua aplikasi tersebut membentuk ekosistem layanan digital terintegrasi yang bergantung pada konsistensi identitas pengguna lintas sistem. Identitas pengurus dan peserta perlu tetap selaras meskipun terjadi perubahan aplikasi, migrasi infrastruktur, atau penyesuaian basis data. Di sinilah watermark citra sebagai lapisan identitas biometrik persisten menawarkan nilai tambah: identitas yang sama dapat ditanamkan pada citra wajah dan diverifikasi di berbagai aplikasi dalam ekosistem yang sama

2. Alur Operasional di Aplikasi Menara Masjid

Pada Aplikasi Menara Masjid, alur usulan penerapan watermark biometrik:

a. Pendaftaran/Pembaruan Profil Pengurus
Pengurus diregistrasi oleh admin; sistem melakukan *face capture* untuk foto profil.
b. Preprocessing dan Pembentukan Payload Citra
di-*preprocess* (cropping, alignment, normalisasi). Payload dibentuk dari Hash(UserID pengurus), SystemID = MENARA, IntegritySignature, dan Timestamp.
c. Embedding Watermark
Payload dikodekan dan disisipkan secara invisible ke dalam citra wajah menggunakan algoritma watermark.
d. Penyimpanan dan Penggunaan Operasional
Citra watermarked disimpan di database biometrik dan dikaitkan dengan entitas pengurus di database aplikasi. Citra itu digunakan di tampilan profil, halaman admin, dan laporan.
e. Audit Pergantian Pengurus dan Riwayat Kepengurusan
Jika terjadi pergantian pengurus, watermark citra pengurus lama dapat diekstraksi untuk verifikasi identitas pada dokumentasi masa lalu. Hal ini memperkuat jejak audit kepengurusan dan mengurangi potensi sengketa terkait pengambil keputusan di masa lalu.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

3. Alur Operasional di Aplikasi Microfinance Masjid

Pada Aplikasi Microfinance Masjid, alur operasionalnya:

a. Registrasi Peserta dan Face Capture
Calon peserta mendaftar, sistem mengambil citra wajah sebagai identitas biometrik utama.
b. Preprocessing dan Payload Generation
Citra diproses (cropping wajah, alignment, normalisasi). Payload dibentuk dari Hash(UserID peserta), SystemID = MICROFINANCE, IntegritySignature, dan Timestamp.
c. Embedding dan Penyimpanan
Payload disisipkan sebagai invisible watermark. Citra watermarked disimpan di database biometrik dan dikaitkan dengan profil peserta, data usaha, serta riwayat pembiayaan.
d. Verifikasi pada Layanan dan Monitoring
Saat monitoring lapangan atau pengajuan lanjutan, citra arsip peserta dapat diverifikasi dengan mengekstrak watermark. Ketidaksesuaian payload dapat mengindikasikan adanya perubahan citra atau upaya penyamaran identitas.
e. Audit Ketika Terjadi Sengketa
Jika terjadi sengketa terkait identitas peserta atau klaim pembiayaan, watermark pada citra arsip dapat diekstraksi sebagai bagian dari proses forensik internal. Payload yang memuat Hash(UserID), SystemID, dan Timestamp membantu memastikan bahwa citra tersebut memang terkait dengan peserta dan waktu pendaftaran tertentu.

Melalui dua alur ini, identitas biometrik di Menara Masjid dan Microfinance Masjid tidak hanya bergantung pada entri database dan berkas administratif, tetapi memiliki lapisan identitas persisten yang tertanam langsung pada citra wajah.

M. Diskusi

Bagian ini membahas implikasi utama dan kontribusi praktis dari kerangka yang diusulkan, sebagaimana dirangkum dalam poin-poin berikut:

1. Watermark citra dapat diposisikan ulang dari sekadar mekanisme hak cipta menjadi identitas biometrik persisten;
2. Pendekatan ini meningkatkan robustness tata kelola identitas terhadap perubahan metadata, basis data, dan infrastruktur;
3. Dengan payload yang terstruktur, watermark dapat mendukung interoperabilitas lintas aplikasi dan jejak audit yang kuat;
4. Penambahan dimensi tracking dan mitigasi deepfake membuat watermark relevan dalam konteks ancaman modern yang memanfaatkan teknologi generatif.

Kerangka ini sejalan dengan transformasi digital pada Aplikasi Menara Masjid BAZNAS [27] dengan penekanan pada keamanan biometrik dan tata kelola identitas wajah, serta menjadi kelanjutan menuju pembahasan teknis keamanan citra biometrik. Namun, masih terdapat sejumlah tantangan:

a. Overhead komputasi untuk embedding–extraction pada skala besar;
b. Trade-off antara kualitas citra, kapasitas payload, dan robustness [1], [2], [6];
c. Ketergantungan pada manajemen kunci dan keamanan modul embed–extract;
d. Perlunya kajian empiris dan pengukuran numerik pada data nyata, termasuk skenario deepfake yang lebih kompleks.

Kerangka ini menyediakan dasar penting yang kuat untuk penelitian lanjutan di bidang implementasi algoritma watermarking berbasis *deep learning* atau *diffusion models*, integrasi dengan modul deteksi *deepfake* dan *anti-spoofing*, serta evaluasi di lingkungan operasional sungguhan sebagai konteks penerapan yang lebih luas dan representatif pada skala multi-masjid dan multi-daerah.

V. KESIMPULAN

Artikel ini mengusulkan kerangka konseptual watermark citra sebagai lapisan identitas biometrik persisten dalam arsitektur tata kelola dan interoperabilitas data wajah. Dengan menanamkan payload identitas *(Hash(UserID), SystemID, IntegritySignature, Timestamp)* langsung pada sinyal citra wajah, sistem tidak lagi sepenuhnya bergantung pada metadata dan basis data sebagai satu-satunya sumber identitas, sekaligus memperkuat integritas data biometrik dan mendukung mekanisme audit jangka panjang. Pendekatan ini memungkinkan interoperabilitas identitas lintas aplikasi dalam ekosistem digital terintegrasi, termasuk Menara Masjid dan Microfinance Masjid, sehingga identitas biometrik tetap dapat diverifikasi meskipun terjadi perubahan sistem, migrasi data, atau ketidaktersediaan basis data.

Selain itu, watermark citra menyediakan mekanisme tambahan untuk pelacakan asal-usul citra, proteksi kepemilikan, serta mitigasi manipulasi berat termasuk indikasi *deepfake* dalam konteks verifikasi biometrik internal. Ke depan, kerangka ini berpotensi dikembangkan menjadi plugin keamanan biometrik lintas sistem, diuji secara eksperimental menggunakan berbagai algoritma watermarking dan skenario serangan, serta diintegrasikan ke dalam kerangka kerja keamanan dan privasi yang lebih luas sesuai dengan standar nasional dan internasional.

REFERENSI

[1] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, dan T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. Morgan Kaufmann, 2008.

[2] M. Barni dan F. Bartolini, *Watermarking Systems Engineering*. New York, NY, USA: Marcel Dekker, 2004.

[3] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2009.

[4] A. K. Jain, A. Ross, dan S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004.

[5] A. K. Jain, K. Nandakumar, dan A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, Article ID 579416, 2008.

[6] Y. Liu, X. Chen, J. Liu, dan X. Wang, "Deep learning for robust digital watermarking: A survey," *Neurocomputing*, vol. 335, pp. 1–16, 2019/2020.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

[7] J. Galbally, S. Marcel, dan J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.
[8] S. Wang, D. Zhang, dan X. Wang, "Digital watermarking for image authentication and integrity verification," *Multimedia Tools and Applications*, vol. 75, pp. 10671–10695, 2016.
[9] ISO/IEC 24745:2011, *Information Technology — Security Techniques — Biometric Information Protection*, International Organization for Standardization, 2011.
[10] A. Juels dan M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, pp. 237–257, 2006.
[11] R. Munir, Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Informatika, 2012.
[12] T. Sutoyo, E. Mulyanto, V. Suhartono, O. D. Nurhayati, dan Wijanarto, *Teori Pengolahan Citra Digital*. Yogyakarta: Andi, 2009.
[13] A. Kadir dan A. Susanto, *Pengolahan Citra: Teori dan Aplikasi*. Yogyakarta: Andi, 2013.
[14] E. Prasetyo, Pengolahan Citra Digital dan Aplikasinya Menggunakan MATLAB. Yogyakarta: Andi, 2011.
[15] [15] R. Munir, "Steganografi dan watermarking pada citra digital," Jurnal Ilmu Komputer dan Teknologi Informasi, vol. X, no. Y, pp. 1–10, 2010.
[16] N. Hidayat dan A. Harjoko, "Pengamanan citra digital menggunakan teknik watermarking berbasis DWT," Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), vol. 4, no. 2, 2015.
[17] S. S. Kusumadewi, "Keamanan biometrik pada sistem identifikasi digital," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 5, no. 3, 2018.
[18] A. Setiawan dan B. Hidayat, "Implementasi watermarking untuk perlindungan integritas citra digital," Jurnal Informatika, vol. 10, no. 1, 2017.
[19] M. K. Khan dan J. Zhang, "Multimodal face and fingerprint biometrics authentication on space-limited tokens," *Neurocomputing*, vol. 71, pp. 3026–3031, 2008 / dan berbagai karya lanjutan terkait watermarking biometrik.
[20] R. Caldelli, F. Filippini, dan R. Becarelli, "Reversible watermarking techniques: An overview and a classification," *EURASIP Journal on Information Security*, vol. 2010, Article ID 134546, 2010.
[21] Badan Siber dan Sandi Negara (BSSN), *Pedoman Keamanan Informasi dan Perlindungan Data Digital*. Jakarta, Indonesia, 2020.
[22] Kementerian Komunikasi dan Informatika Republik Indonesia, *Strategi Nasional Keamanan Siber dan Perlindungan Data*. Jakarta, Indonesia, 2021.
[23] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016.
[24] Republik Indonesia, Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Jakarta, Indonesia, 2022.
[25] ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements, International Organization for Standardization, 2022.
[26] ISO/IEC 27701:2019, Security Techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidelines, International Organization for Standardization, 2019.
[27] M. R. Kusuma, "Transformasi Digital Pengelolaan Masjid Berbasis Inovasi Sistem Informasi dan Regulasi Nasional: Studi Evaluatif terhadap Aplikasi Menara Masjid BAZNAS," *Bangkit Indonesia*, vol. 14, no. 2, Okt. 2025, doi: 10.52771/bangkitindonesia.v14i2.447.

DOI : 10.52771/bangkitindonesia.v15i1.483
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267