ANALISIS KEAMANAN SISTEM AUTENTIKASI BIOMETRIK IRIS MENGGUNAKAN METODE CANCELABLE BIOMETRICS UNTUK PERLINDUNGAN TEMPLATE

Intan Nur Janah, Adila Muqtashida, Putri Dwi Manggali,
Muhammad Rifki Hidayatullah, Muhammad Fadhil Dwisaputra, Ibnu Mas'ud
Informatika, Universitas Islam Negeri Sultan maulana Hasanuddin Banten
Jl. Syekh Nawawi Al-Bantani, Sukawana, Curug, Kota Serang, 42171, Indonesia
intannurjanah3001@gmail.com

ABSTRAK

Perkembangan sistem identifikasi digital mendorong penggunaan autentikasi biometrik iris karena Tingkat akurasi dan keunikannya yang tinggi. Namun, sifat data biometrik yang permanen menimbulkan permasalahan serius terkait keamanan dan privasi, terutama resiko kebocoran template biometrik yang berpotensi direkonstruksi. Permasalahan utama dalam sistem autentikasi iris Adalah kerentanan template terhadap serangan rekonstruksi serta keterbatasan mekanisme perlindungan data yang bersifat *revocable*. Penelitian ini bertujuan untuk merancang dan mengevaluasi sistem autentikasi biometrik iris yang lebih aman melalui penerapan metode *Cancelable Biometrics* tanpa menurunkan kinerja autentikasi secara signifikat. Metode penelitian dilakukan secara eksperimental menggunakan dataset CASIA-IrisV3 dan UBIRIS.v2 melalui tahapan *preprocessing*, ekstraksi fitur iris menggunakan Gabor wavelet, serta transformasi template berbasis *randomized projection* dan *hashing transformation.* Hasil penelitian menunjukkan bahwa metode *Cancelable Biometrics* mampu mempertahankan tingkat akurasi sistem sebesar 95,34% dengan peningkatan signifikan pada aspek keamanan. Pengujian *non-invertibility, revocability,* dan *unlinkability* membuktikan bahwa template hasil transformasi aman dari rekonstruksi, dapat diterbitkan ulang, dan tidak dapat ditautkan lintas sistem.

Kata kunci : *biohashing, biometrik iris, biometrik yang dapat dibatalkan, keamanan template biometrik, proyeksi acak.*

1. PENDAHULUAN

Perkembangan teknologi identifikasi digital menempatkan sistem autentikasi biometrik iris sebagai salah satu komponen kunci dalam arsitektur keamanan modern. Jika dibandingkan dengan metode berbasis pengetahuan, seperti kata sandi, maupun metode berbasis kepemilikan, seperti kartu atau token fisik yang relatif mudah dicuri atau disalahgunakan, biometrik iris menawarkan keunggulan yang signifikan. Pola iris bersifat sangat unik pada setiap individu, relatif stabil sepanjang hayat, serta memiliki kompleksitas tinggi yang membuatnya hampir tidak mungkin direplikasi secara identik oleh pihak lain[1]. Karakteristik ini menjadikan iris kerap dipandang sebagai "standar emas" dalam sistem biometrik, sehingga diadopsi secara luas pada berbagai sektor strategis, mulai dari kontrol perbatasan, sistem keimigrasian, hingga layanan perbankan digital.

Namun demikian, keunggulan tersebut juga membawa konsekuensi serius. Berbeda dengan kredensial digital yang dapat diganti sewaktu-waktu, data biometrik bersifat permanen. Ketika data iris mengalami kebocoran, identitas biometrik pengguna berpotensi terkompromi secara permanen, karena karakteristik fisiologis tersebut tidak dapat diubah atau diperbarui seperti halnya kata sandi[2]. Salah satu persoalan utama dalam sistem autentikasi iris adalah kerentanan template biometrik terhadap serangan rekonstruksi. Template numerik yang disimpan dalam basis data, seperti iris code atau representasi fitur lainnya, pada dasarnya masih menyimpan informasi struktural dari iris asli. Apabila template ini berhasil diakses oleh pihak tidak berwenang, penyerang dengan kemampuan komputasi yang memadai dapat memanfaatkan algoritma tertentu untuk merekonstruksi citra iris yang menyerupai bentuk aslinya.

Kekhawatiran terhadap risiko ini semakin meningkat seiring munculnya inisiatif global seperti proyek *Worldcoin* yang melakukan pengumpulan data iris dalam skala masif. Meskipun mengusung tujuan verifikasi identitas global, proyek semacam ini memicu perdebatan luas terkait etika pengelolaan data, kedaulatan informasi, serta potensi penyalahgunaan identitas, khususnya di negara berkembang [3]. Dalam konteks Indonesia, permasalahan ini diperumit oleh adanya ketimpangan antara pesatnya adopsi teknologi biometrik dan kesiapan regulasi hukum yang mengaturnya. Tanpa kerangka regulasi yang adaptif serta tingkat literasi digital yang memadai, masyarakat berada dalam posisi yang rentan terhadap eksploitasi data sensitif yang dampaknya sulit dipulihkan [4]. Berbagai penelitian sebelumnya telah berupaya mengatasi tantangan tersebut melalui pendekatan teknis yang beragam. Pada tahap akuisisi dan ekstraksi fitur, penggunaan sensor kamera inframerah (IR) yang dikombinasikan dengan algoritma *Scale Invariant Feature Transform* (SIFT) terbukti mampu menghasilkan fitur iris yang stabil, meskipun terjadi variasi rotasi, skala, maupun kondisi pencahayaan [5]. Pendekatan ini meningkatkan keandalan sistem dari sisi akurasi pengenalan.

Namun, tingginya akurasi ekstraksi fitur belum secara otomatis menjamin perlindungan privasi. Oleh karena itu, penelitian mutakhir mulai mengarah pada pendekatan yang lebih berorientasi pada *privacy-preserving.* Salah satunya adalah pemanfaatan *Neural Style Transfer* (NST) untuk menyamarkan tekstur asli iris dengan gaya visual tertentu, sehingga data yang tersimpan tidak lagi secara langsung merepresentasikan biometrik manusia, tetapi tetap dapat digunakan secara efektif dalam proses pencocokan oleh system [6].

Selain itu, konsep *Cancelable Biometrics* semakin mendapat perhatian karena menawarkan mekanisme keamanan yang lebih adaptif. Melalui teknik regularisasi eigenfeature dan transformasi tertentu, template biometrik dapat dibuat bersifat *revocable*, sehingga dapat ditarik kembali dan diterbitkan ulang apabila terjadi kebocoran, tanpa harus mengganti data iris asli pengguna[7]. Pendekatan ini menjadi semakin relevan mengingat berbagai evaluasi pada perangkat komersial saat ini masih menunjukkan adanya celah terhadap serangan *spoofing*, rekayasa citra, maupun manipulasi digital lainnya [8].

Berdasarkan celah yang teridentifikasi dalam literatur, penelitian ini bertujuan untuk merumuskan kerangka kerja sistem autentikasi biometrik iris yang tidak hanya unggul dari sisi akurasi, tetapi juga memiliki ketahanan siber yang tinggi melalui perlindungan template biometrik yang berlapis. Kebaruan penelitian ini terletak pada integrasi hibrida antara teknik transformasi fitur berbasis *Cancelable Biometrics* dan strategi mitigasi risiko yang mempertimbangkan konteks regulasi perlindungan data di Indonesia.

Berbeda dengan penelitian sebelumnya yang cenderung menitikberatkan pada performa algoritma secara terpisah, penelitian ini mengaitkan aspek teknis ekstraksi dan transformasi fitur dengan dimensi etika siber serta kepatuhan hukum. Dengan pendekatan tersebut, penelitian ini diharapkan dapat memberikan kontribusi dalam perancangan sistem identitas digital yang tidak hanya akurat dan aman secara teknis, tetapi juga memenuhi prinsip *non-invertibility* dan selaras dengan standar perlindungan data pribadi yang berlaku.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Berbagai penelitian telah dilakukan untuk mengatasi permasalahan keamanan pada sistem biometrik [7] mengusulkan metode RP-RegSt dan RP-RegSb yang mengkombinasikan teknik random permutation dengan *regularized eigenfeature extraction.* Hasil penelitian tersebut menunjukkan bahwa penerapan permutasi acak tidak hanya mampu melindungi template biometrik, tetapi juga memberikan peningkatan akurasi pengenalan pada dataset CASIA-V1 dan UBIRIS.v1.

Selanjutnya, [2] mengembangkan skema *cancelable biometrics* yang bersifat *modality-independent* melalui transformasi vector fitur acak. Pendekatan ini menghasilkan *pseudo-identifier* yang tahan terhadap serangan rekonstruksi dan dapat diterapkan pada berbagai jenis biometrik tanpa ketergantungan pada satu modalitas tertentu. Pendekatan berbeda ditawarkan oleh [9] yang memanfaatkan *Neural Style Transfer* (NST) untuk menyamarkan tekstur asli iris ke dalam gaya visual tertentu. Temuan mereka menunjukkan bahwa tekstur asli iris ke dalam gaya visual tertentu. Temuan mereka menunjukkan bahwa penggunaan fitur gaya mampu memberikan ketahanan yang lebih baik terhadap variasi rotasi dan perubahan presfektif dibandingkan fitur CNN konvensional.

Dalam konteks transformasi fitur, [10] menerapkan Teknik *Random Projection* yang dikombinasikan dengan *Discrete Fourier Transformation* (DFT) untuk melindungi template biometrik biner. Metode ini terbukti memenuhi prinsip *revocability* dan *non-invertibility* pada sistem biometric sidik jari.

Dari sisi implementasi, [8] melakukan kajian keamanan biometrik pada perangkat *smartphone* dan menegaskan bahwa perlindungan template berbasis *cancelable biometrics* merupakan kebutuhan penting untuk mencegah manipulasi digital maupun serangan fisik pada sensor. Sementara, [11] memperluas konsep perlindungan privasi ke biometrik wajah melalui penerapan *soft-biometric privacy enhancement*, yang menunjukkan bahwa perlindungan identitas tetap dapat dicapai tanpa mengurangi fungsionalitas utama sistem autentikasi.

2.2. Keamanan Sistem Biometrik Iris

Sistem biometrik berbasis iris dikenal sebagai salah satu metode identifikasi yang sangat andal, mengingat pola tekstur iris bersifat unik dan relatif stabil pada setiap individu [1]. Meski demikian, persoalan utama tidak terletak pada akurasinya, melainkan pada keamanan template biometrik yang disimpan. Sejumlah studi terbaru mengungkapkan bahwa template iris yang tidak dilindungi dengan baik rentan terhadap berbagai ancaman siber, seperti pencurian identitas hingga manipulasi data, terutama pada perangkat berbasis mobile [8]. Di satu sisi, pemanfaatan sensor berteknologi tinggi mampu meningkatkan kualitas akuisisi citra iris, namun di sisi lain juga menuntut penerapan mekanisme dan protokol privasi yang lebih ketat agar data biometrik tidak disalahgunakan[12].

2.3. Konsep *Cancelable Biometrics*

Cancelable Biometrics merupakan pendekatan keamanan yang bekerja dengan menerapkan transformasi satu arah (*one-way transformation*) pada data biometrik sebelum proses penyimpanan. Pendekatan ini dirancang agar template biometrik dapat dicabut dan digenerasi ulang apabila terjadi

kebocoran, tanpa mengharuskan pengguna melakukan perekaman ulang data iris aslinya [2], [13]. Teknik seperti BioHashing dan Randomized Projection berperan penting dalam menghasilkan template yang bersifat *non-invertible*, sehingga data hasil transformasi tidak dapat direkonstruksi kembali menjadi iris code awal [11]. Selain itu, penerapan prinsip simetri dalam proses transformasi fitur turut meningkatkan ketahanan template terhadap berbagai serangan inversi [10].

2.4. Teknik Ekstraksi Fitur dan Perlindungan Privasi

Pada tahap ekstraksi fitur, algoritma seperti Gabor Wavelet dan Eigenfeature Regularization dimanfaatkan untuk memperoleh karakteristik iris yang bersifat unik serta memiliki tingkat diskriminasi yang tinggi [7]. Seiring meningkatnya perhatian terhadap isu privasi, sejumlah pendekatan terkini mulai mengadopsi Neural Style Transfer (NST) sebagai mekanisme penyamaran visual iris, dengan tetap mempertahankan kemampuan sistem dalam melakukan proses pencocokan [6]. Selain itu, kajian berbasis Deep Learning mengindikasikan bahwa kinerja sistem biometrik iris sangat dipengaruhi oleh kualitas segmentasi citra, terutama ketika diuji pada berbagai dataset publik seperti CASIA dan UBIRIS [9][10].

2.5. Tantangan Etika dan Regulasi di Indonesia

Penerapan sistem biometrik dalam skala besar, seperti yang dilakukan pada proyek Worldcoin, telah memunculkan berbagai perdebatan terkait etika siber serta isu kedaulatan data, baik di tingkat global maupun nasional [3]. Dalam konteks Indonesia, penggunaan teknologi biometrik perlu disesuaikan dengan ketentuan Undang-Undang Perlindungan Data Pribadi (UU PDP). Rendahnya tingkat literasi digital masyarakat, disertai dengan potensi celah dalam regulasi dan penegakan hukum, dapat memperbesar risiko penyalahgunaan data sensitif [4]. Oleh sebab itu, sinergi antara perlindungan teknis melalui pendekatan Cancelable Biometrics dan kepatuhan terhadap kerangka hukum yang berlaku menjadi faktor penting dalam membangun ekosistem identitas digital yang aman, berkelanjutan, dan dapat dipercaya [13].

3. METODE PENELITIAN

3.1. Desain Penelitian

Penelitian ini menerapkan desain eksperimen kuantitatif berbasis simulasi dengan pendekatan analisis komparatif. Rancangan penelitian difokuskan untuk mengevaluasi sejauh mana metode *Cancelable Biometrics* mampu melindungi template iris tanpa menurunkan kinerja autentikasi secara signifikan. Untuk tujuan tersebut, dilakukan perbandingan antara dua skenario utama, yaitu sistem yang menggunakan template iris asli tanpa perlindungan dan sistem yang menggunakan template hasil transformasi *cancelable*. Perbandingan ini bertujuan untuk menilai dampak distorsi fitur terhadap tingkat akurasi serta peningkatan keamanan system [11].

3.2. Data dan Sumber Data

Eksperimen ini memanfaatkan data sekunder berupa dataset citra iris publik yang telah banyak digunakan dan diakui dalam penelitian biometrik, yaitu CASIA-IrisV3 dan UBIRIS.v2. Pemilihan kedua dataset ini didasarkan pada ketersediaan *ground truth* yang jelas serta keberagaman kualitas citra, termasuk variasi pencahayaan, oklusi kelopak mata, dan noise, yang merepresentasikan kondisi nyata dalam implementasi sistem biometric [12]. Secara keseluruhan, simulasi dilakukan menggunakan 2.000 citra iris yang mencakup sejumlah subjek berbeda.

3.3. Tahapan Prepocessing dan Ekstraksi Fitur

Sebelum proses transformasi dilakukan, citra iris melalui beberapa tahapan preprocessing untuk memastikan kualitas data yang optimal.

Tahap pertama adalah segmentasi, di mana batas pupil dan iris dilokalisasi menggunakan Daugman Integro-Differential Operator. Metode ini dipilih karena terbukti mampu mendeteksi batas iris secara konsisten pada sekitar 95% data uji [5].

Selanjutnya, dilakukan proses normalisasi dengan menerapkan Daugman's Rubber Sheet Model, yang mengubah wilayah iris dari koordinat kartesian ke koordinat polar. Proses ini menghasilkan citra iris ternormalisasi dengan ukuran standar 512 × 64 piksel.

Tahap akhir adalah ekstraksi fitur, di mana karakteristik unik iris diekstraksi menggunakan Gabor Wavelet Filter untuk menghasilkan representasi biner berupa iris code dengan panjang 2048 bit [12].

3.4. Protokol Cancelable Biometrics

Tahapan utama dalam penelitian ini adalah penerapan skema Cancelable Biometrics berbasis kombinasi Randomized Projection dan Hashing Transformation. Proses transformasi dilakukan melalui beberapa langkah.

Pertama, iris code asli sepanjang 2048 bit digunakan sebagai masukan. Selanjutnya, fitur tersebut diproyeksikan ke ruang fitur baru menggunakan matriks acak yang berfungsi sebagai kunci transformasi (T-key) dan diproses melalui fungsi pemetaan non-linier menggunakan teknik BioHashing. Pendekatan ini dirancang untuk membentuk fungsi satu arah (one-way function) yang memenuhi prinsip non-invertibility, sehingga template asli tidak dapat direkonstruksi kembali dari hasil transformasi [11], [13].

Hasil akhir dari proses ini berupa template cancelable yang memiliki nilai Hamming Distance rata-rata sebesar 0,50 terhadap template asli, yang mengindikasikan tingkat keacakan dan perlindungan yang optimal.

3.5. Instrumen Evaluasi dan Analisis Data

Kinerja sistem dievaluasi menggunakan metrik standar yang umum digunakan dalam penelitian biometrik untuk memastikan validitas dan reliabilitas hasil. Evaluasi akurasi dilakukan dengan menghitung nilai Accuracy, False Acceptance Rate (FAR), dan False Rejection Rate (FRR). Penentuan ambang batas autentikasi didasarkan pada nilai Equal Error Rate (EER) terendah [10]. Selain itu, pengujian keamanan dilakukan melalui beberapa indikator utama. Aspek non-invertibility diuji dengan mensimulasikan serangan rekonstruksi, seperti teknik hill-climbing, untuk memastikan bahwa template asli tidak dapat dipulihkan dari template hasil transformasi [11]. Aspek revocability dievaluasi dengan mengukur kemampuan sistem dalam menghasilkan template baru yang tidak berkorelasi ketika kunci transformasi diubah [12]. Sementara itu, unlinkability diuji untuk memastikan bahwa template yang dihasilkan tidak dapat dilacak lintas basis data, dengan target nilai korelasi kurang dari 0,10 [10].

4. HASIL DAN PEMBAHASAN

4.1. Instrumen Evaluasi dan Analisis Data

Tahap *preprocessing* yang mencakup proses segmentasi, normalisasi, dan pengurangan noise berhasil diterapkan pada seluruh dataset. Hasil evaluasi menunjukkan bahwa metode berbasis *integro-differential operator* mampu mendeteksi batas pupil dan iris secara konsisten pada sekitar 95% citra uji. Meskipun pada beberapa citra dengan kondisi pencahayaan yang kurang optimal ditemukan ketidaktepatan segmentasi, dampak tersebut dapat diminimalkan pada tahap normalisasi selanjutnya. Penerapan *Daugman's rubber sheet model* berhasil mentransformasikan citra iris ke dalam koordinat polar dengan ukuran 512 × 64 piksel, sehingga struktur fitur menjadi seragam sebelum proses ekstraksi dilakukan.

4.2. Hasil Ekstraksi Fitur Iris

Proses ekstraksi fitur menggunakan Gabor wavelet filter menghasilkan representasi biner berupa iris code dengan panjang 2048 bit. Analisis statistik terhadap hasil ekstraksi menunjukkan tingkat kemiripan intra-class yang tinggi, yaitu sebesar 0,85, serta tingkat kemiripan inter-class yang rendah, yakni 0,17. Perbedaan yang signifikan antara kedua nilai tersebut mengindikasikan bahwa fitur iris yang dihasilkan memiliki daya diskriminasi yang baik, sehingga dataset dinilai valid dan layak digunakan untuk pengujian sistem keamanan biometrik.

4.3. Hasil Penerapan Metode Cancelable Biometrics

Penerapan metode *Cancelable Biometrics* dilakukan dengan mengombinasikan teknik *randomized projection* dan *hashing transformation*. Pengaturan parameter kunci transformasi (*T-key*) serta faktor distorsi menghasilkan template biometrik yang bersifat non-visual dan tidak dapat dipetakan kembali ke *iris code* asli.

Hasil pengukuran menunjukkan bahwa nilai *Hamming Distance* (HD) antara template asli dan template hasil transformasi berada pada rentang 0,48 hingga 0,52. Rentang nilai ini mencerminkan tingkat keacakan atau entropi yang tinggi, yang menandakan bahwa transformasi berhasil menghilangkan keterkaitan langsung dengan data biometrik asli.

4.4. Hasil Pengujian Performa Sistem

Evaluasi performa sistem dilakukan dengan membandingkan kondisi sebelum transformasi (template asli) dan setelah transformasi (*cancelable template*). Ringkasan hasil pengujian disajikan pada Tabel I.

Tabel 1. Performa Akurasi dan Error Rate

Kondisi	Akurasi	FAR	FRR
Template Asli	98,12%	0,021	0,034
Template Cancelable	95,34%	0,028	0,051

Hasil pengujian menunjukkan adanya penurunan akurasi sebesar sekitar 2,78% setelah penerapan transformasi cancelable. Penurunan ini dinilai masih berada dalam batas yang dapat diterima, mengingat peningkatan signifikan pada aspek keamanan dan perlindungan data biometrik yang diperoleh.

4.5. Hasil Pengujian Aspek Keamanan

Pengujian keamanan dilakukan untuk mengevaluasi tiga aspek utama, yaitu non-invertibility, revocability, dan unlinkability. Pada pengujian non-invertibility, simulasi serangan rekonstruksi menggunakan metode hill-climbing tidak menghasilkan keberhasilan pemulihan citra iris, dengan tingkat keberhasilan 0%. Hasil ini menunjukkan bahwa template hasil transformasi aman dari upaya rekonstruksi data biometrik asli.

Aspek revocability diuji dengan mengubah kunci transformasi (T-key). Hasilnya, sistem mampu menghasilkan template baru dengan nilai Hamming Distance rata-rata sebesar 0,50 terhadap template sebelumnya, tanpa menunjukkan korelasi teknis yang berarti. Sementara itu, pengujian unlinkability pada basis data yang berbeda menghasilkan nilai korelasi yang sangat rendah, yaitu di bawah 0,10. Temuan ini mengonfirmasi bahwa template biometrik yang dihasilkan tidak dapat digunakan untuk melacak identitas pengguna lintas sistem.

4.6. Pembahasan

Analisis Kompromi antara Akurasi dan Keamanan (Trade-off): Hasil eksperimen menunjukkan bahwa penerapan metode *Cancelable Biometrics* menyebabkan penurunan tingkat akurasi dari 98,12% menjadi 95,34%. Secara teknis, penurunan sekitar 2,78% ini merupakan konsekuensi logis dari proses distorsi fitur yang dilakukan melalui *randomized projection*. Transformasi tersebut secara

sengaja mengubah struktur *iris code* agar tidak lagi dapat dikenali, baik secara visual maupun melalui analisis algoritmik, oleh pihak yang tidak berwenang. Namun, sebagaimana dikemukakan oleh Singh dkk. [11], penurunan akurasi dalam skala kecil merupakan kompromi yang wajar untuk memperoleh tingkat perlindungan privasi yang jauh lebih tinggi. Dengan tingkat akurasi yang masih berada di atas 95%, sistem tetap memenuhi kriteria operasional untuk aplikasi keamanan tingkat tinggi, seperti layanan perbankan digital atau kontrol akses pada fasilitas terbatas. Temuan ini menunjukkan bahwa algoritma yang digunakan mampu menjaga keseimbangan antara fungsi autentikasi dan kebutuhan perlindungan data biometrik.

Ketahanan terhadap Serangan Rekonstruksi (Non-Invertibility): Salah satu hasil paling signifikan dalam penelitian ini adalah keberhasilan sistem dalam memenuhi prinsip *non-invertibility*, yang ditunjukkan oleh tingkat keberhasilan rekonstruksi sebesar 0%. Pada sistem biometrik konvensional, kebocoran basis data template dapat membuka peluang bagi penyerang untuk melakukan proses inversi guna memulihkan citra iris asli pengguna. Sebaliknya, penerapan *hashing transformation* pada penelitian ini menghasilkan template yang bersifat satu arah (*one-way*), sehingga tidak memungkinkan proses pemulihan data biometrik asli. Hasil ini memperkuat temuan Ragendhu S. P. [13], yang menyatakan bahwa penggunaan transformasi fitur berbasis vektor acak mampu menciptakan lapisan proteksi yang sangat sulit ditembus, bahkan dengan serangan berbasis *hill-climbing* atau teknik optimasi lainnya. Dengan demikian, meskipun terjadi kebocoran basis data, informasi yang diperoleh penyerang tidak memiliki nilai biologis maupun identitas yang bermakna.

Efektivitas Mekanisme Revobility: Salah satu keterbatasan utama sistem biometrik adalah sifat data fisiologis yang tidak dapat diganti. Berbeda dengan kata sandi, biometrik secara alami bersifat permanen. Namun, hasil pengujian *revocability* menunjukkan bahwa permasalahan ini dapat diatasi melalui pengelolaan kunci transformasi (*T-key*). Ketika kunci transformasi diubah, sistem mampu menghasilkan template baru dengan tingkat korelasi yang sangat rendah terhadap template sebelumnya, yang ditunjukkan oleh nilai *Hamming Distance* rata-rata sebesar 0,50. Hal ini berarti bahwa kompromi terhadap satu template tidak berdampak pada keamanan template yang diterbitkan ulang. Temuan ini sejalan dengan pendekatan yang diusulkan oleh Rajasekar dkk. [12], di mana fleksibilitas manajemen kunci berperan sebagai solusi praktis atas sifat permanen data biometrik, sehingga konsep biometrik dapat mendekati mekanisme "reset kredensial" pada sistem autentikasi tradisional.

Perlindungan Privasi Lintas Platform melalui Unlinkability: Hasil pengujian *unlinkability* menunjukkan bahwa nilai korelasi antar basis data berada di bawah ambang 0,10, yang menandakan bahwa template biometrik tidak dapat ditautkan lintas sistem. Temuan ini memiliki implikasi penting dalam konteks perlindungan privasi pengguna. Tanpa mekanisme *unlinkability*, penyedia layanan yang berbeda berpotensi menggabungkan data biometrik untuk melacak aktivitas individu secara lintas platform. Dengan tingkat korelasi yang sangat rendah, template iris yang digunakan pada satu layanan, seperti perbankan digital, tidak dapat dicocokkan dengan template pada layanan lain, misalnya sistem kesehatan, meskipun berasal dari individu yang sama. Pendekatan ini memberikan jaminan privasi yang lebih kuat dan secara langsung menjawab kekhawatiran etis yang sering dikemukakan terhadap proyek biometrik berskala besar, termasuk Worldcoin, yang kerap dikritik karena potensi pelacakan identitas secara global [3], [4].

Rekomendasi Implementasi pada Perangkat Komersial: Berdasarkan stabilitas nilai *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR), metode yang diusulkan dinilai layak untuk diimplementasikan pada perangkat dengan keterbatasan sumber daya, seperti smartphone. Meskipun perangkat komersial modern telah mengadopsi autentikasi biometrik, sebagian besar masih menyimpan template dalam bentuk yang relatif rentan terhadap manipulasi digital. Hasil penelitian ini mendukung rekomendasi Yeovandi dkk. [8] yang menekankan pentingnya perlindungan template sebagai standar keamanan wajib pada sistem biometrik perangkat bergerak. Integrasi metode *Cancelable Biometrics* berpotensi meningkatkan kepercayaan pengguna dalam melakukan transaksi finansial maupun menyimpan data sensitif pada perangkat pribadi.

4.7. Analisis Akhir

Secara keseluruhan, hasil penelitian ini menunjukkan bahwa penerapan metode *Cancelable Biometrics* pada sistem autentikasi iris tidak hanya memungkinkan secara teknis, tetapi juga sangat penting dalam konteks keamanan digital modern. Sistem berhasil mempertahankan tingkat akurasi di atas 95% sekaligus memberikan perlindungan penuh terhadap serangan rekonstruksi template. Dengan menggabungkan performa autentikasi yang tinggi, mekanisme *revocability*, serta jaminan *unlinkability*, pendekatan ini menawarkan solusi komprehensif untuk membangun sistem identitas biometrik yang aman, adaptif, dan selaras dengan prinsip perlindungan privasi.

5. KESIMPULAN DAN SARAN

Penelitian ini bertujuan merancang dan mengevaluasi sistem autentikasi biometrik iris yang tidak hanya memiliki tingkat akurasi tinggi, tetapi juga mampu memberikan perlindungan yang kuat terhadap risiko kebocoran data biometrik permanen. Berdasarkan hasil eksperimen dan pembahasan, penerapan metode *Cancelable Biometrics* berbasis

randomized projection dan *hashing transformation* terbukti efektif dalam melindungi template iris tanpa menurunkan performa autentikasi secara signifikan. Meskipun terjadi penurunan akurasi sebesar ±2,78%, sistem tetap mempertahankan tingkat akurasi di atas 95%, yang masih memenuhi standar operasional untuk aplikasi keamanan tingkat tinggi. Lebih lanjut, pengujian aspek keamanan menunjukkan bahwa template hasil transformasi bersifat non-invertible dengan tingkat keberhasilan rekonstruksi sebesar 0%, mampu diterbitkan ulang melalui mekanisme *revocability*, serta aman dari pelacakan lintas basis data melalui pemenuhan prinsip *unlinkability*. Temuan ini menegaskan bahwa integrasi perlindungan template merupakan komponen esensial dalam pengembangan sistem identitas digital modern, khususnya dalam konteks meningkatnya pemanfaatan biometrik iris di Indonesia. Untuk penelitian selanjutnya, pendekatan ini dapat dikembangkan dengan mengintegrasikan mekanisme *liveness detection*, optimasi komputasi untuk perangkat berdaya rendah, serta pengujian pada skenario implementasi nyata guna memperkuat ketahanan sistem terhadap serangan biometrik yang semakin kompleks.

DAFTAR PUSTAKA

[1] K. K. Prakasha, S. Member, and U. Sumalatha, "Privacy-Preserving Techniques in Biometric Systems : Approaches and Challenges," *IEEE Access*, vol. 13, no. February, pp. 32584–32616, 2025, doi: 10.1109/ACCESS.2025.3541649.

[2] T. Thomas and S. Emmanuel, "Cancelable Biometric Template Generation Using Random Feature Vector Transformations," vol. 12, no. February, 2024.

[3] U. Hasanuddin, "Triwikrama: Jurnal Ilmu Sosial," vol. 8, no. 8, pp. 1–11, 2025.

[4] J. Hukum and C. Justitia, "No Title," vol. 4, no. 2, pp. 90–104, 2024.

[5] S. Lock, S. Deteksi, and I. Mata, "Technology Sciences Insights Journal," no. 2023, 2025.

[6] C. Zhang *et al.*, "The Historical Evolution and Significance of Multiple Sequence Alignment in Molecular Structure and Function Prediction," 2024.

[7] M. Mishra, S. Panda, S. Barik, A. Sarkar, and D. V. Singh, "Antibiotic Resistance Profile , Outer Membrane Proteins , Virulence Factors and Genome Sequence Analysis Reveal Clinical Isolates of Enterobacter Are Potential Pathogens Compared to Environmental Isolates," vol. 10, no. February, pp. 1–13, 2020, doi: 10.3389/fcimb.2020.00054.

[8] R. Implementasi, F. Yeovandi, E. Prasetyo, P. Studi, T. Informasi, and U. I. Batam, "JTIM : Jurnal Teknologi Informasi dan Multimedia Evaluasi Keamanan Sistem Autentikasi Biometrik," vol. 7, no. 1, pp. 133–148, 2025.

[9] M. Wang, E. F. E. Bozkir, and E. Kasneci, "Iris Style Transfer : Enhancing Iris Recognition with Style Features and Privacy Preservation through Neural Style Transfer Iris Style Transfer : Enhancing Iris Recognition with Style Features and Privacy Preservation through Neural Style Transfer," vol. 8, no. 2, 2026, doi: 10.1145/3729413.

[10] P. Punithavathi and S. Geetha, "Random Projection-based Cancelable Template Generation for Sparsely Distributed Biometric Patterns," vol. 7, no. 3, pp. 877–886, 2017, doi: 10.11591/ijeecs.v7.i3.pp877-886.

[11] P. Melzi *et al.*, "Cancelable Face Biometrics With Soft-Biometric Privacy Enhancement," vol. 13, no. July, 2025, doi: 10.1109/ACCESS.2025.3590989.

[12] C. Iris and K. Binding, "SS symmetry A New Design for Alignment-Free Chaffed," 2019, doi: 10.3390/sym11020164.

[13] C. Science, "PROCESS OF FINGERPRINT AUTHENTICATION USING," vol. 24, no. 4, pp. 537–564, 2023.