Implementasi Kriptografi Visual untuk Pengamanan Data Biometrik

Samy Muhammad Haikal 13522151 [1,2]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13522151@std.stei.itb.ac.id, [2]samymhaikal82@gmail.com

***Abstract*— Data biometrik, seperti sidik jari dan wajah, merupakan identitas unik yang bersifat permanen dan tidak dapat diganti apabila terjadi kebocoran data. Saat ini standar industri adalah menyimpan data biometrik dalam bentuk *feature vector*. Meskipun *feature vector* memang tidak memiliki informasi tentang data biometrik asli, beberapa penelitian menunjukkan bahwa data yang berbentuk *feature vector* ini masih dapat direkonstruksi untuk mendapatkan data biometrik yang sensitif. Hal ini dapat menimbulkan masalah jika terjadi kebocoran data dan dapat menjadi celah bagi vendor untuk menyalahgunakan data biometrik pengguna. Makalah ini mengusulkan implementasi skema Kriptografi Visual untuk mengamankan penyimpanan data biometrik. Dengan skema ini data yang disimpan akan benar-benar tidak bisa direkonstruksi kembali sehingga akan meningkatkan keamanan data biometrik pengguna.**

***Keywords*— Biometrik, Keamanan Siber, Vektor Embedding, Kriptografi Visual.**

I. PENDAHULUAN

Teknologi biometrik, seperti pengenalan wajah (*face recognition*) dan sidik jari, telah menjadi standar *de facto* dalam sistem autentikasi modern, mulai dari akses perangkat seluler hingga sistem keamanan perbankan. Popularitas ini didorong oleh kenyamanan pengguna dan anggapan bahwa biometrik lebih aman daripada kata sandi tradisional. Namun, berbeda dengan kata sandi atau token yang dapat diganti apabila terjadi peretasan, data biometrik bersifat intrinsik dan permanen pada diri individu. Sifat ketidaktergantikan (*non-repudiable*) ini menciptakan risiko keamanan yang kritikal; apabila data biometrik bocor, identitas pengguna akan terkompromi selamanya tanpa kemungkinan untuk diperbarui.

Saat ini, praktik standar industri untuk memitigasi risiko penyimpanan data adalah dengan tidak menyimpan gambar mentah. Sebagai gantinya, sistem mengekstraksi fitur unik dari data biometrik menjadi representasi matematis yang disebut *feature vector* atau *embedding*. Selama bertahun-tahun, *feature vector* dianggap aman karena sifatnya yang searah dan tidak dapat dibaca secara visual oleh manusia. Namun, perkembangan pesat dalam bidang *Deep Learning* dan *Generative Adversarial Networks* (GANs) telah mematahkan asumsi tersebut. Penelitian terbaru menunjukkan bahwa *feature vector* yang tersimpan dalam basis data rentan terhadap serangan rekonstruksi (*model inversion attack*), di mana penyerang dapat memulihkan kembali wajah atau sidik jari asli dari vektor tersebut dengan tingkat akurasi yang tinggi.

***Gambar 1** Contoh rekonstruksi wajah asli dari feature vector*
Sumber: [2]

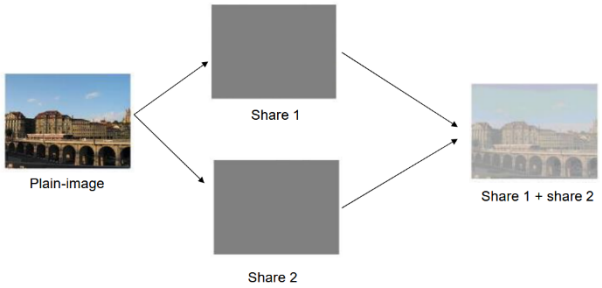
Risiko ini menuntut adanya lapisan keamanan tambahan yang dapat menjamin kerahasiaan data bahkan jika basis data utama diretas. Kriptografi Visual, sebuah skema pembagian rahasia yang diperkenalkan oleh Naor dan Shamir pada tahun 1994, menawarkan solusi matematis untuk masalah ini. Konsep dasar dari Kriptografi Visual adalah memecah sebuah informasi menjadi beberapa bagian berupa pola acak (*noise*). Informasi asli hanya dapat dipulihkan apabila seluruh shares digabungkan kembali, sementara satu share saja tidak memberikan informasi apa pun mengenai data aslinya.

Makalah ini mengusulkan implementasi teknik Kriptografi Visual untuk mengamankan penyimpanan feature vector biometrik. Dengan menerapkan skema ini, data yang disimpan oleh penyedia layanan hanyalah berupa random noise yang secara matematis mustahil untuk direkonstruksi kembali menjadi data biometrik asli tanpa memiliki share kunci yang dipegang oleh pengguna. Pendekatan ini diharapkan dapat menutup celah keamanan pada penyimpanan biometrik konvensional dan melindungi privasi pengguna dari ancaman kebocoran data maupun penyalahgunaan oleh pihak internal.

II. DASAR TEORI

A. Kriptografi Visual

Kriptografi Visual (VC) adalah teknik kriptografi yang mengenkripsi informasi dengan suatu cara sehingga dekripsi cukup dilakukan dengan mempersepsi informasi melalui indra penglihatan (mata). Teknik ini diperkenalkan oleh Naor dan Shamir dalam makalah yang berjudul "*Visual Cryptography*" di dalam jurnal *Eurocrypt'94*. Konsep dasar kriptografi visual adalah membagi sebuah citra rahasia menjadi beberapa bagian acak yang disebut *shares*. Secara individual, setiap *share* tidak mengungkapkan informasi apa pun tentang citra asli dan tampak sebagai random noise. Informasi asli hanya dapat dipulihkan apabila seluruh shares digabungkan kembali.



Gambar 2.1 *Ilustrasi cara kerja kriptografi visual*
Sumber: [6]

Kriptografi visual tradisional berbasis biner (hitam-putih) menggunakan operasi logika XOR atau penumpukan transparansi, sementara itu implementasi modern pada citra grayscale atau berwarna sering menggunakan skema *Additive Secret Sharing* berbasis aritmatika modular. Metode ini memungkinkan pemulihan citra secara lossless (tanpa penurunan kualitas).

Dalam skema ini, jika I adalah matriks citra asli dan S1 adalah matriks acak (share pertama) dengan dimensi yang sama, maka share kedua (S2) dihitung menggunakan operasi pengurangan modulo 256:

$$S_2 = (I - S_1) \; mod \; 256$$

Untuk merekonstruksi citra asli, penerima cukup menjumlahkan kedua *share* tersebut:

$$I = (S_1 + S_2) \; mod \; 256$$

Keamanan skema ini terletak pada sifat keacakan . Karena dihasilkan dari distribusi seragam, maka juga akan terlihat acak secara statistik. Hal ini memenuhi prinsip *Perfect Secrecy* menurut teori informasi Shannon, di mana intersepsi terhadap salah satu *share* saja tidak memberikan keuntungan probabilitas apa pun bagi penyerang untuk menebak citra asli.

B. FaceNet

FaceNet, yang dikembangkan oleh peneliti Google (Schroff et al., 2015), adalah sistem pengenalan wajah berbasis Deep Convolutional Neural Network (CNN). Berbeda dengan pendekatan tradisional yang menggunakan *hand-crafted features*, FaceNet memetakan wajah secara langsung dari piksel ke dalam ruang Euclidean berdimensi rendah (biasanya 128-dimensi). Vektor hasil pemetaan ini disebut sebagai embedding.

Inti dari arsitektur FaceNet adalah penggunaan Triplet Loss Function. Fungsi ini bekerja dengan mengambil tiga gambar input: Anchor (A), Positive (P - gambar orang yang sama dengan A), dan Negative (N - gambar orang yang berbeda).

Tujuan dari pelatihan jaringan adalah untuk memastikan bahwa jarak Euclidean antara Anchor dan Positive lebih kecil daripada jarak antara Anchor dan Negative dengan margin α:

$$\left|\left|f(x^a) - f(x^p)\right|\right|_2^2 + \alpha < \left|\left|f(x^a) - f(x^n)\right|\right|_2^2$$

Dalam makalah ini, *FaceNet* digunakan sebagai ekstraktor fitur untuk membandingkan fitur foto yang dikirim saat ini dan foto yang didekripsi dari *share*.

C.Rekonstruksi wajah dari feature vector

Salah satu miskonsepsi umum dalam keamanan biometrik adalah anggapan bahwa fungsi ekstraksi fitur bersifat satu arah (one-way), menyerupai fungsi hashing kriptografi, sehingga wajah asli tidak dapat dikembalikan dari feature vector yang tersimpan. Asumsi ini didasarkan pada fakta bahwa proses embedding melakukan reduksi dimensi yang membuang sebagian besar data piksel asli. Namun, serangkaian penelitian dalam satu dekade terakhir membuktikan bahwa embedding wajah sebenarnya mempertahankan karakteristik geometris dan fotometrik yang cukup untuk merekonstruksi wajah asli dengan tingkat akurasi yang mengkhawatirkan [1].

Teknik ini dikenal sebagai Model Inversion Attack (MIA). Pada penelitian awal oleh Fredrikson et al., didemonstrasikan bahwa penyerang dapat mengeksploitasi informasi nilai kepercayaan dari API pengenalan wajah untuk melakukan inversi dan memulihkan gambar wajah target, meskipun hasilnya masih berupa citra yang kabur [2]. Mahendran dan Vedaldi kemudian memperkuat temuan ini dengan menunjukkan bahwa representasi internal pada Deep Convolutional Neural Networks (CNN) menyimpan informasi visual yang akurat secara fotografis pada berbagai layernya, memungkinkan rekonstruksi citra melalui optimasi gradien [1].

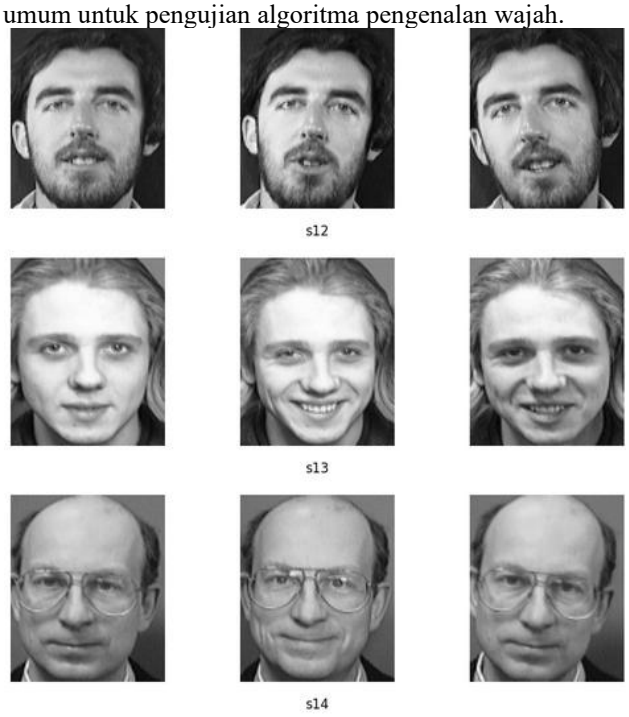
Ancaman ini berevolusi secara signifikan dengan diperkenalkannya teknik berbasis *Generative Adversarial Networks* (GANs). Zhang et al. mengusulkan metode *Generative Model-Inversion* (GMI) yang memanfaatkan pengetahuan prior tentang wajah manusia yang dipelajari oleh GAN. Alih-alih merekonstruksi wajah dari nol, penyerang menggunakan generator GAN untuk menghasilkan wajah sintetik yang secara visual realistis dan memiliki feature vector yang identik dengan target [3]. Dengan metode ini, wajah hasil rekonstruksi tidak hanya mirip secara matematis, tetapi juga memiliki kualitas visual yang tinggi sehingga dapat dikenali oleh mata manusia.

Lebih lanjut, penelitian terbaru pada tahun 2024 oleh Shahreza et al. menunjukkan bahwa serangan ini menjadi

semakin efektif dengan bantuan *Face Foundation Models*. Dengan menggunakan teknik *adapter*, penyerang dapat merekonstruksi wajah dari *embedding model* kotak hitam dengan detail yang presisi, membuktikan bahwa mekanisme perlindungan berbasis model saja tidak lagi memadai [4]. Fakta bahwa feature vector terbukti rentan terhadap serangan inversi mendasari urgensi penerapan Kriptografi Visual pada lapisan penyimpanan. Dalam sistem yang diusulkan ini, perlindungan diterapkan pada data mentah sebelum ekstraksi fitur dilakukan, sehingga memutus rantai serangan inversi sejak sumbernya.

D. Database

Dataset yang digunakan dalam pengujian sistem ini adalah AT&T Database of Faces (sebelumnya dikenal sebagai ORL Database of Faces). Dataset ini dikelola oleh AT&T Laboratories Cambridge dan merupakan standar umum untuk pengujian algoritma pengenalan wajah.



Gambar 2.2 *Sampel data dari AT&T Database of Faces*
Sumber: [8]

Dataset ini terdiri dari 40 subjek yang berbeda. Untuk setiap subjek, terdapat 10 citra wajah yang diambil dengan variasi kondisi, termasuk perbedaan pencahayaan, ekspresi wajah (mata terbuka/tertutup, tersenyum/tidak), serta aksesoris wajah (kacamata). Seluruh citra memiliki format PGM (Portable Gray Map) dengan resolusi 92x112 piksel. Variasi dalam dataset ini sangat penting untuk menguji ketahanan (robustness) dari sistem biometrik yang diusulkan, terutama dalam skenario Multi-Shot Enrollment menggunakan metode Centroid.

III. IMPLEMENTASI

Untuk menyelasikan maslah keamanan penyimpanan data biometrik, penulis merancang sebuah system di mana data biometrik yang disimpan hanya berupa *share* dari gambar asli yang tidak bisa direkonstruksi ulang untuk mendapatkan wajah asli pengguna. Citra wajah hanya akan direkonstruksi sesaat di memory volatile (RAM) Ketika proses verifikasi berlangsung, dan segera dihapus setelah vector fitur diekstraksi dan dibandingkan.

A. Alur Sistem

Alur kerja sistem dibagi menjadi dua fase utama: Fase Registrasi dan Fase Autentikasi.

1. Fase Registrasi

Pada fase ini, sistem mengambil 3 sampel wajah pengguna untuk membentuk identitas yang stabil. Setiap sampel dienkripsi menjadi dua share.

Alur proses registrasi:

1. **Input**: Pengguna memberikan 3 citra wajah (I1 ,I2,I3) dengan variasi pose minor.
2. **Enkripsi**: Setiap citra In dipecah menggunakan Kriptografi Visual menjadi ShareAn (disimpan di Server) dan ShareBn (diberikan ke Token Pengguna/Smart Card).
3. **Validasi Kualitas**: Sistem melakukan dekripsi sementara untuk memastikan wajah dapat dikenali oleh FaceEngine.
4. **Kalkulasi Centroid**: Vektor fitur dari ketiga citra dirata-rata untuk menghasilkan vektor referensi pusat (Centroid) yang disimpan sebagai template utama.

2. Fase Autentikasi

Pada fase ini, sistem memverifikasi apakah citra input (dari kamera atau probe) cocok dengan share yang tersimpan.

Alur proses autentikasi:

1. **Retrieval**: Sistem mengambil Share A dari database dan menerima Share B dari pengguna.
2. **Rekonstruksi**: Kedua share dijumlahkan (Modulo 256) untuk menghasilkan citra wajah rekonstruksi (Irec).
3. **Ekstraksi**: FaceEngine mengubah Irec menjadi vektor 128-dimensi.
4. **Decision**: Jarak Euclidean dihitung antara vektor baru dengan Vektor Centroid. Jika jarak < 0.50, akses diberikan.

B. Modul

Implementasi terdiri dari tiga modul utama yaitu RGBVisualCryptoGPU, ImageUtils, dan FaceEngine. Berikut adalah penjelasan mendetail tentang ketiga modul yang diimplementasikan

1. RGBVisualCryptoGPU

Kelas ini berfungsi untuk melakukan operasi enkripsi dan dekripsi citra menggunakan algoritma Kriptografi Visual berbasis *Additive Secret Sharing* dengan aritmatika Modulo 256. Kelas ini dirancang khusus untuk akselerasi perangkat keras, di mana seluruh manipulasi matriks dilakukan secara paralel di dalam memori GPU (VRAM) menggunakan tipe data torch.Tensor.

Kelas ini menggunakan PyTorch untuk operasi tensor dan CUDA untuk komputasi paralel.

No	Method	Keterangan

1	encrypt(self, tensor_images)	Menerima input berupa tensor citra dan menghasilkan share A dan Share B
2	decrypt(self, share_a, share_b)	Metode ini merekonstruksi citra asli dengan menjumlahkan share A dan share B

2. ImageUtils

Kelas ini berfungsi sebagai utilitas pembantu (helper) untuk menangani proses input-output (I/O) dan pra-pemrosesan citra standar sebelum masuk ke pipeline GPU. Fungsi utamanya adalah memastikan konsistensi format warna dan resolusi citra.

Kelas ini menggunakan OpenCV (cv2) untuk pembacaan citra, NumPy untuk manipulasi array, dan Requests/PIL untuk menangani input dari URL.

No	Method	Keterangan
1	load_rgb_image(image_path, width)	Memuat citra dari jalur lokal (local path) atau URL internet.

3. FaceEngine

Kelas ini berfungsi sebagai mesin biometrik utama yang menangani deteksi wajah dan ekstraksi fitur (embedding). Berbeda dengan implementasi standar, kelas ini dioptimalkan untuk Batch Processing, memungkinkan pemrosesan ratusan citra sekaligus dalam satu kali operasi matriks.

Kelas ini menggunakan pustaka *facenet-pytorch* yang mencakup model MTCNN untuk deteksi wajah dan InceptionResnetV1 untuk ekstraksi fitur, serta memanfaatkan akselerasi GPU.

No	Method	Keterangan
1	preprocess_batch(self, image_paths)	Membaca sekumpulan path file citra dan mengonversinya menjadi daftar objek gambar yang siap diproses menjadi tensor.
2	get_embeddings_batch(self, img_tensor_batch)	Mengubah batch tensor citra wajah menjadi vektor fitur 512-dimensi. Proses ini mencakup normalisasi (whitening) dan resizing ke 160x160 piksel sebelum diteruskan ke model ResNet.
3	detect_and_embed_batch(self, pil_images_list)	Mendeteksi lokasi wajah menggunakan MTCNN, memotong area wajah, dan mengekstraksi vektor fiturnya dalam mode batch.
4	compute_distance_matrix(self, ref_vector, batch_vectors)	Menghitung jarak Euclidean antara satu vektor referensi dengan sekumpulan besar vektor lain secara simultan menggunakan operasi matriks

C. Test script

Fungsi run_fast_evaluation adalah skrip pengujian utama yang dirancang untuk mensimulasikan skenario autentikasi massal (batch authentication) pada seluruh dataset. Skrip ini mengintegrasikan modul Kriptografi Visual dan Face Engine untuk mengukur kinerja keamanan dan akurasi sistem.

Alur kerja skrip ini dibagi menjadi empat tahapan logis:

1. Pre-loading Dataset ke Memori GPU

Langkah pertama adalah memuat seluruh dataset citra wajah (400 citra dari 40 subjek) ke dalam memori (RAM) dan mengonversinya menjadi Tensor PyTorch yang disimpan di VRAM GPU.

- Tujuan: Mengeliminasi bottleneck input-output (I/O) disk yang lambat saat proses iterasi.
- Proses: Citra dibaca, diubah ke RGB, dan ditumpuk menjadi satu tensor berdimensi (400, 3, 112, 92).

2. Multi-Shot Enrollment & Kalkulasi Centroid

Untuk setiap subjek dalam loop pengujian, sistem melakukan simulasi pendaftaran yang:

- Sampling: Mengambil 3 citra pertama dari subjek tersebut.
- Enkripsi-Dekripsi: Ketiga citra diproses melalui RGBVisualCryptoGPU untuk mensimulasikan kondisi riil penyimpanan data terproteksi.
- Pembentukan Centroid: Vektor fitur dari ketiga citra hasil dekripsi diekstraksi dan dirata-rata untuk membentuk satu vektor referensi pusat yang stabil.

3. Vectorized Matching Strategy

Skrip ini melakukan perbandingan vektor secara massal:

- Probe Selection: Memilih seluruh sisa citra dalam database (397 citra) sebagai probe (pengunjung yang mencoba masuk).
- Batch Distance Computation: Menghitung Jarak Euclidean antara Vektor Centroid target dengan seluruh 397 vektor probe sekaligus dalam satu operasi matriks GPU. Teknik ini mempercepat waktu komputasi secara eksponensial dibandingkan metode CPU sekuensial.

4. Evaluasi Keamanan dan Akurasi

Hasil jarak dibandingkan dengan threshold (0.50) untuk menentukan apakah data biometric cocok atau tidak. Dilakukan validasi untuk semua data pada dataset dan dihitung akurasi, presisi, dan recall.

Skrip ini mengembalikan DataFrame berisi statistik akurasi dan jumlah pelanggaran keamanan (false positives) untuk setiap subjek, yang digunakan untuk analisis akhir.

IV. EKSPERIMEN

Eksperimen dilakukan untuk mengevaluasi kinerja sistem pengenalan wajah yang terintegrasi dengan skema Kriptografi Visual. Evaluasi dilakukan pada total 15.880 percobaan akses, yang terdiri dari pengujian terhadap pengguna sah dan penyusup. Eksperimen dilakukan menggunakan GPU T4 dari google colab. Seluruh proses pencocokan vektor fitur dilakukan menggunakan Euclidean Distance dengan batas ambang (threshold) ketat sebesar 0.50. Fokus utama analisis adalah mengukur keseimbangan antara keamanan sistem dan kenyamanan pengguna dalam skenario blind-authentication di mana citra referensi disimpan dalam bentuk terenkripsi.

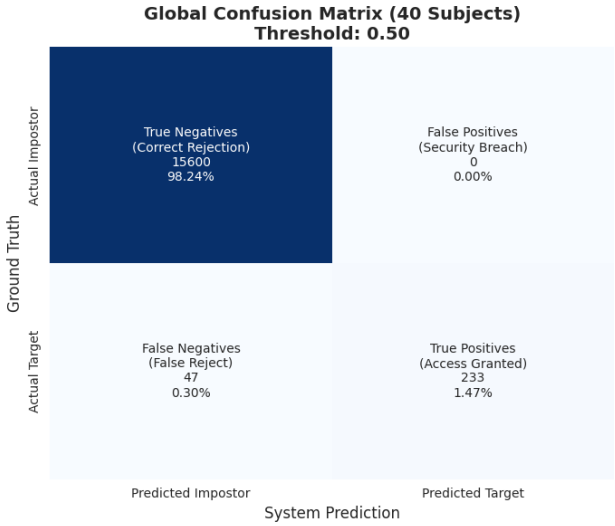
Hasil analisis keamanan kuantitatif menunjukkan bahwa sistem tidak pernah memvalidasi wajah untuk orang yang berbeda. Hal ini ditunjukkan oleh angka False Positive (FP) sebesar 0. Statistik ini mengonfirmasi bahwa vektor fitur yang diekstraksi dari citra hasil rekonstruksi visual cryptography tetap mempertahankan karakteristik unik yang cukup kuat untuk membedakan antar-individu secara presisi.

```
======================================
DETAIL PERFORMA BIOMETRIK
======================================
Total Percobaan Akses : 15,880
--------------------------------------
User Asli Diterima (TP)    : 233 / 280 (Recall: 83.21%)
User Asli Ditolak (FN)     : 47 (Masalah Kenyamanan)
--------------------------------------
Impostor Ditolak (TN)      : 15600 / 15600
Impostor Masuk (FP)        : 0 (Masalah Keamanan)
======================================

==================================================
LAPORAN PERFORMA SISTEM (GPU ACCELERATED)
==================================================
Threshold Keamanan     : 0.5
Rata-rata Akurasi      : 99.70%
Total Security Breaches: 0 (False Positives)
Rata-rata Breach/User  : 0.00
==================================================
```

Gambar 4.1 *Detail performa sistem biometric*
Sumber: Dokumentasi Pribadi

Namun, sistem terkadang masih akan menolak pengguna yang valid (*false negatives*). Meskipun penolakan ini tidak merusak keamanan, ini akan mengharuskan pengguna melakukan pengambilan citra ulang yang mengurangi kenyamanan pengguna dalam pemakaian sistem.



Gambar 4.2 *Confusion matrix*
Sumber: Dokumentasi Pribadi

Berdasarkan *confusion matrix* di atas dapat dilihat bahwa sistem mampu menolak seluruh 15.600 percobaan akses ilegal dengan tepat dan berhasil memverifikasi 233 akses pengguna asli. Nilai 0 pada kuadran *False Positives* (kanan atas) menunjukkan bahwa sistem memiliki tingkat keamanan absolut pada threshold 0.50, di mana tidak ada satupun penyusup yang berhasil menembus sistem, meskipun masih terdapat 47 kasus penolakan terhadap pengguna asli yang perlu mencoba ulang.

V. KESIMPULAN

Berdasarkan rangkaian eksperimen yang telah dilakukan, dapat disimpulkan bahwa integrasi metode RGB Visual Cryptography pada sistem biometrik wajah mampu memberikan jaminan keamanan yang valid. Sistem terbukti mencapai tingkat keamanan absolut (*zero false acceptance*) pada threshold 0.50, menjadikannya solusi yang ideal untuk aplikasi yang memprioritaskan privasi data dan integritas akses di atas segalanya.

Meskipun demikian, system terkadang masih akan menolak pengguna asli yang mengharuskan pengguna mengambil ulang gambar wajahnya. Hal ini akanmengurangi kenyamanan pengguna dalam menggunakan system tetapi tidak akan berpengaruh terhadap keamanan system.

VI. LAMPIRAN

Runbook:
https://colab.research.google.com/drive/1nFTixc4qE2Oy2x5KJ7e8oQfec7-QhT81?usp=sharing .

VII. UCAPAN TERIMA KASIH

Dengan penuh rasa syukur, penulis ingin mengucapkan puji dan syukur kepada Tuhan Yang Maha Esa atas segala rahmat, karunia, serta taufik dan hidayah-Nya, yang telah

memandu dan memberikan keberkahan sehingga penulis berhasil menyelesaikan makalah berjudul " Penerapan Algoritma A* dalam Penyelesaian Sliding Puzzle". Makalah ini disusun sebagai bagian dari tugas mata kuliah Kriptografi IF4020.

Penulis juga mengucapkan terima kasih yang setinggi-tingginya kepada Bapak Dr. Ir. Rinaldi Munir, M.T., sebagai dosen pengajar dalam mata kuliah Kriptografi IF4020. Terima kasih atas dedikasi, bimbingan, dan pengajaran yang telah diberikan selama satu semester ini, memberikan kontribusi besar dalam pembentukan pemahaman kami sebagai mahasiswa.

REFERENCES

[1] A. Mahendran and A. Vedaldi, "Understanding Deep Image Representations by Inverting Them," arXiv preprint arXiv:1412.0035, 2014.

[2] M. Fredrikson, S. Jha, and T. Ristenpart, "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), 2015.

[3] Y. Zhang, R. Jia, H. Pei, W. Wang, B. Li, and D. Song, "The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks," arXiv preprint arXiv:1911.07135, 2020.

[4] H. O. Shahreza, A. George, and S. Marcel, "Face Reconstruction from Face Embeddings using Adapter to a Face Foundation Model," arXiv preprint arXiv:2411.03960, 2024.

[5] Rinaldi Munir, “Kriptografi Visual, Teori dan Aplikasinya (Bagian 1)”, https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/38-Kriptografi-Visual-Bagian1-2025.pdf diakses pada tanggal 26 Desember 2026.

[6] Rinaldi Munir, “Kriptografi Visual, Teori dan Aplikasinya (Bagian 2)”, https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/39-Kriptografi-Visual-Bagian2-2025.pdf diakses pada tanggal 26 Desember 2026.

[7] C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[8] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," in *Proceedings of the 2nd IEEE Workshop on Applications of Computer Vision*, Sarasota, FL, USA, 1994.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 Desember 2025

Samy Muhammad Haikal 13522151