ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.5 No.1 Tahun 2026
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-5 2026
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2026

Pemanfaatan Teknik Steganografi LSB dan Kriptografi AES sebagai Token Autentikasi pada Sistem Kehadiran Gym DsFit

Utilization of LSB Steganography Technique and AES Cryptography as Authentication Tokens in the DsFit Gym Attendance System

Andrian Lusmana[1], Muhammad Akmal Hafiz[2], Yudi Gunawan[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]andrianlusmana794@gmail.com*, [2]akmall.hafizzz@gmail.com*, [3]yudigunawan223@gmail.com*

Abstract

Conventional attendance authentication systems in public facilities, such as DsFit Gym, often face security vulnerabilities in the form of identity manipulation and misuse of access rights. This study proposes the development of an innovative digital token-based authentication system that combines two layers of security: Advanced Encryption Standard (AES-128) cryptography and Least Significant Bit (LSB) steganography. The main objective of this study is to secure member credentials by encrypting them into ciphertext before embedding them into profile photo images, thus creating an invisible and secure access key. The research method is carried out by designing an encoder algorithm for data embedding and a decoder for attendance validation. Based on quantitative testing results, the resulting image tokens show superior visual quality with a Peak Signal-to-Noise Ratio (PSNR) value reaching 89.05 dB and a Mean Square Error (MSE) of 0.0001, indicating that image distortion is very minimal and difficult to detect by human vision. In addition, functional testing proves that the system is able to decrypt and verify member identities with a 100% accuracy rate from the test samples. This hybrid cryptosystem approach has proven effective as a private, secure, and hard-to-fake authentication solution.

Keywords: *Image Steganography, Least Significant Bit, Advanced Encryption Standard, Authentication System, Data Security*

Abstrak

Sistem autentikasi kehadiran konvensional pada fasilitas publik, seperti Gym DsFit, sering kali menghadapi celah keamanan berupa manipulasi identitas dan penyalahgunaan hak akses. Penelitian ini mengusulkan pengembangan sistem autentikasi inovatif berbasis token digital yang menggabungkan dua lapisan keamanan: kriptografi *Advanced Encryption Standard* (AES-128) dan steganografi *Least Significant Bit* (LSB). Tujuan utama penelitian ini adalah mengamankan kredensial anggota dengan mengenkripsinya menjadi *ciphertext* sebelum disisipkan ke dalam citra foto profil, sehingga menciptakan kunci akses yang tidak terlihat (*invisible*) dan aman. Metode penelitian dilakukan dengan merancang algoritma *encoder* untuk penyisipan data dan *decoder* untuk validasi kehadiran. Berdasarkan hasil pengujian kuantitatif, token citra yang dihasilkan menunjukkan kualitas visual superior dengan nilai *Peak Signal-to-Noise Ratio* (PSNR) mencapai 89,05 dB dan *Mean Square Error* (MSE) sebesar 0,0001, yang mengindikasikan bahwa distorsi citra sangat minim dan sulit dideteksi oleh indra penglihatan manusia. Selain itu, pengujian fungsional membuktikan sistem mampu mendekripsi dan memverifikasi identitas anggota dengan tingkat akurasi 100% dari sampel uji. Pendekatan *hybrid cryptosystem* ini terbukti efektif sebagai solusi autentikasi yang privat, aman, dan sulit dipalsukan.

Kata kunci: *Steganografi Citra*, *Least Significant Bit*, *Advanced Encryption Standard*, *Sistem Autentikasi*, *Keamanan Data*

Pendahuluan

Perkembangan teknologi informasi yang masif telah menempatkan keamanan data sebagai prioritas utama dalam ekosistem digital, terutama untuk melindungi kerahasiaan informasi dari akses yang tidak sah [1], [2]. Salah satu mekanisme pertahanan yang efektif adalah steganografi, yakni seni menyembunyikan pesan

rahasia ke dalam media penampung seperti citra digital sehingga keberadaannya tersamar secara visual [3]. Dalam ranah *image steganography*, metode *Least Significant Bit* (LSB) menjadi teknik yang paling dominan digunakan karena kemampuannya menyisipkan bit informasi pada lapisan bit terendah piksel tanpa mendegradasi kualitas citra secara signifikan, yang juga sering dimanfaatkan untuk perlindungan hak cipta (*copyright*) [4]. Namun, penggunaan steganografi semata dinilai memiliki celah keamanan, karena apabila algoritma penyisipan diketahui, pesan rahasia dapat diekstraksi dengan mudah oleh pihak ketiga.

Guna menutupi celah tersebut, konsep keamanan berlapis (*layered security*) melalui integrasi kriptografi mutlak diperlukan. Algoritma *Advanced Encryption Standard* (AES) dikenal sebagai standar enkripsi modern yang memiliki ketahanan tinggi terhadap serangan *brute force*, menjadikannya pendamping ideal untuk mengamankan data sebelum disisipkan [5]. Implementasi AES-128 terbukti mampu menjaga integritas file sensitif dengan performa komputasi yang efisien [6]. Berbagai penelitian terdahulu memperlihatkan bahwa kombinasi teknik LSB dengan enkripsi mampu meningkatkan derajat keamanan secara drastis, baik dalam konteks pengamanan pesan teks maupun aset informasi korporat [7], [8]. Sinergi ini memastikan bahwa meskipun *stego-image* berhasil dianalisis, informasi di dalamnya tetap tidak dapat dibaca tanpa kunci dekripsi yang valid.

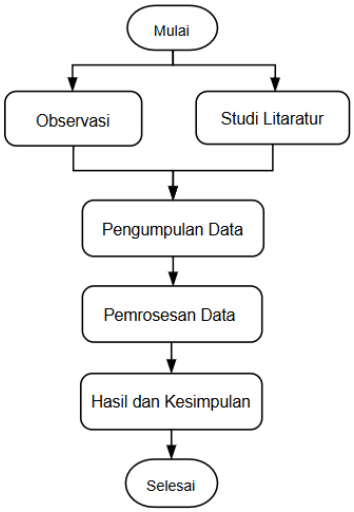
Meskipun integrasi steganografi dan kriptografi telah banyak diteliti, terdapat kesenjangan (*gap*) signifikan dari sisi implementasi fungsional dan ketahanan teknis. Mayoritas riset saat ini masih berkutat pada fungsi dasar penyembunyian file pesan untuk komunikasi rahasia [9] atau sekadar pengujian parameter teknis seperti ketahanan terhadap kompresi media sosial dan variasi bit [10], [11]. Masih jarang ditemukan penelitian yang mengeksplorasi penggunaan *image steganography* sebagai instrumen autentikasi aktif pada sistem *Internet of Things* (IoT) atau sistem kehadiran fisik, padahal metode ini memiliki potensi besar sebagai pengganti token konvensional [12]. Ketiadaan implementasi steganografi sebagai token akses inilah yang menjadi peluang penelitian yang mendesak untuk digarap.

Berdasarkan analisis celah dari penelitian tersebut, Penelitian ini berfokus pada pengembangan sistem kehadiran Gym DsFit untuk mengatasi kerentanan metode konvensional. Solusi yang diusulkan adalah pemanfaatan teknik *image steganography* LSB yang diperkuat enkripsi AES sebagai token autentikasi. Kebaruan penelitian ini terletak pada transformasi citra digital menjadi 'kunci digital' aktif untuk verifikasi kehadiran otomatis. Sistem ini menjamin keamanan dan privasi tinggi, di mana validasi akses bergantung sepenuhnya pada keberhasilan dekripsi kredensial yang tersembunyi dalam *stego-image*.

Metode Penelitian

Alur Tahapan Penelitian

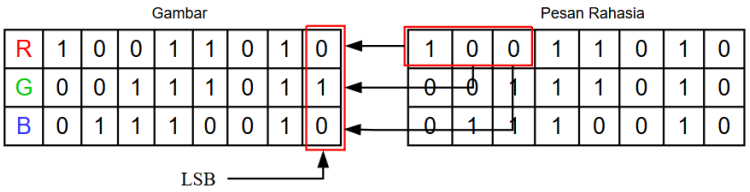
Alur penelitian dilaksanakan melalui serangkaian tahapan teknis terstruktur mulai dari akuisisi data citra anggota hingga validasi sistem akhir. Kerangka kerja ini mengacu pada model pengembangan sistem keamanan hibrida yang mengintegrasikan aspek kerahasiaan (*confidentiality*) dan imperceptibilitas (*imperceptibility*). Langkah-langkah penelitian yang dilakukan secara berurutan disajikan dalam diagram alur pada Gambar 1.



Gambar 1: Diagram Alur Penelitian

Least Significant Bit

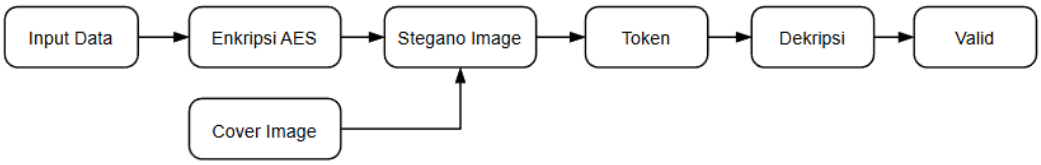
Penelitian ini dirancang dengan pendekatan eksperimental untuk membangun mekanisme autentikasi token digital yang aman dan tahan terhadap analisis visual. Fokus teknis penelitian ini terletak pada pemanfaatan karakteristik bit paling tidak signifikan (*Least Significant Bit*) pada struktur piksel RGB 24-bit untuk menyisipkan muatan data terenkripsi. Sebagaimana diilustrasikan pada Gambar 2, strategi manipulasi bit ke-8 dipilih karena perubahan nilai intensitas warna sebesar satu poin desimal pada kanal warna merah, hijau, atau biru tidak memberikan dampak perseptual yang signifikan bagi sistem penglihatan manusia, namun cukup untuk menyimpan informasi biner secara persisten [13].



Gambar 2: Ilustrasi Manipulasi Bit pada Posisi LSB untuk Penyisipan Data

Mekanisme Enkripsi Data

Mekanisme pengamanan data dirancang dengan menggabungkan dua lapisan pertahanan digital. Pada lapisan pertama, data kredensial anggota (ID dan Nama) diamankan menggunakan algoritma enkripsi simetris AES-128 dengan mode operasi *Cipher Block Chaining* (CBC). Penerapan mode CBC dengan *Initialization Vector* (IV) acak bertujuan untuk menghilangkan korelasi antara *plaintext* dan *ciphertext*, sehingga pola data input yang identik tidak menghasilkan pola output yang sama [14]. Pada lapisan kedua, *ciphertext* hasil enkripsi disisipkan ke dalam citra *cover* menggunakan teknik substitusi LSB. Integrasi kedua algoritma ini menjamin bahwa token citra yang dihasilkan tidak hanya menyembunyikan keberadaan pesan, tetapi juga melindungi isi pesan dari upaya ekstraksi ilegal. Alur proses enkripsi dan penyisipan data digambarkan pada Gambar 3.



Gambar 3: Skema Alur Enkripsi AES-CBC dan Penyisipan LSB

Metode Pengukuran Kualitas Citra

Untuk memvalidasi tingkat imperceptibilitas citra hasil steganografi, penelitian ini menggunakan parameter kuantitatif *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). MSE digunakan untuk menghitung rata-rata kuadrat kesalahan antara citra asli (*cover image*) dengan citra hasil sisipan (*stego image*). Nilai MSE yang semakin mendekati nol menunjukkan tingkat kemiripan yang semakin tinggi, sebagaimana ditunjukkan pada Persamaan (1):

$$MSE = \frac{1}{M\ x\ N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - S(i,j)]^2 \quad (1)$$

Di mana M dan N merepresentasikan dimensi lebar dan tinggi citra, I(i,j) adalah nilai piksel citra asli, dan S(i,j) adalah nilai piksel citra steganografi. Selanjutnya, kualitas visual diukur dalam satuan desibel (dB) menggunakan PSNR yang dirumuskan pada Persamaan (2):

$$PSNR = 10 \cdot \log_{10}(\frac{(Cmax)^2}{MSE}) \quad (2)$$

Di mana C_{max} bernilai 255 untuk citra 8-bit. Nilai PSNR yang tinggi (biasanya di atas 40 dB) mengindikasikan bahwa distorsi pada citra sangat rendah dan sulit dideteksi mata manusia.

Hasil dan Pembahasan

Implementasi sistem diuji menggunakan dataset citra digital yang merepresentasikan foto profil anggota Gym DsFit. Citra masukan yang digunakan berasal dari format standar *Joint Photographic Experts Group* (JPEG/JPG). Mengingat karakteristik kompresi *lossy* pada format JPG yang berpotensi merusak integritas data pada level bit, sistem dirancang untuk melakukan konversi format otomatis menjadi *Portable Network Graphics* (PNG) sebelum proses penyisipan dilakukan. Format PNG dipilih karena mendukung kompresi *lossless*, menjamin bahwa bit-bit pesan yang disisipkan pada posisi *Least Significant Bit* (LSB) tetap persisten dan tidak mengalami perubahan nilai saat disimpan. Spesifikasi teknis dari sampel citra yang digunakan dalam pengujian ini dirangkum pada Gambar 4.

(a) *(b)* *(c)* *(d)*

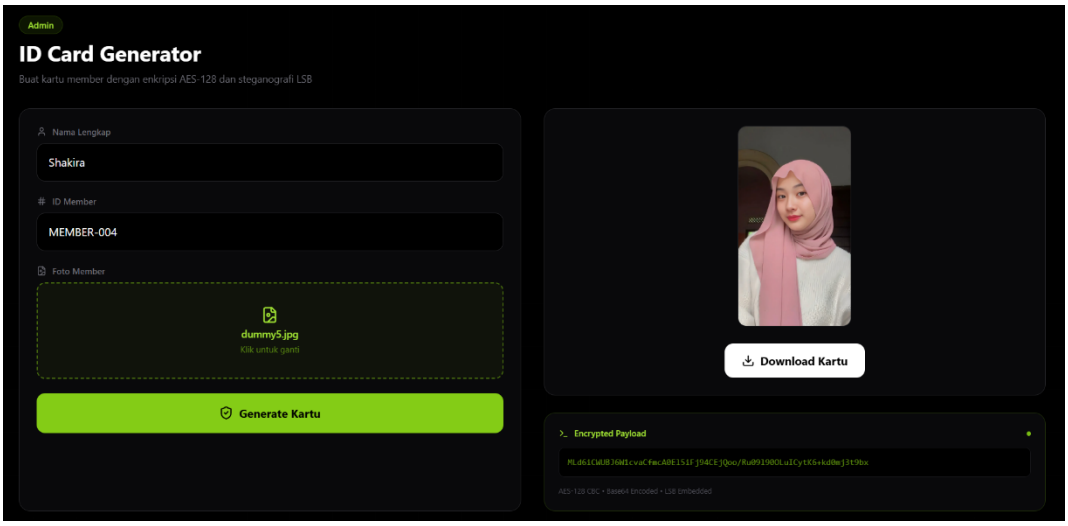
Gambar 4: Sample Foto Member Gym DSFfit

Tabel 1: Spesifikasi Dataset Citra Uji

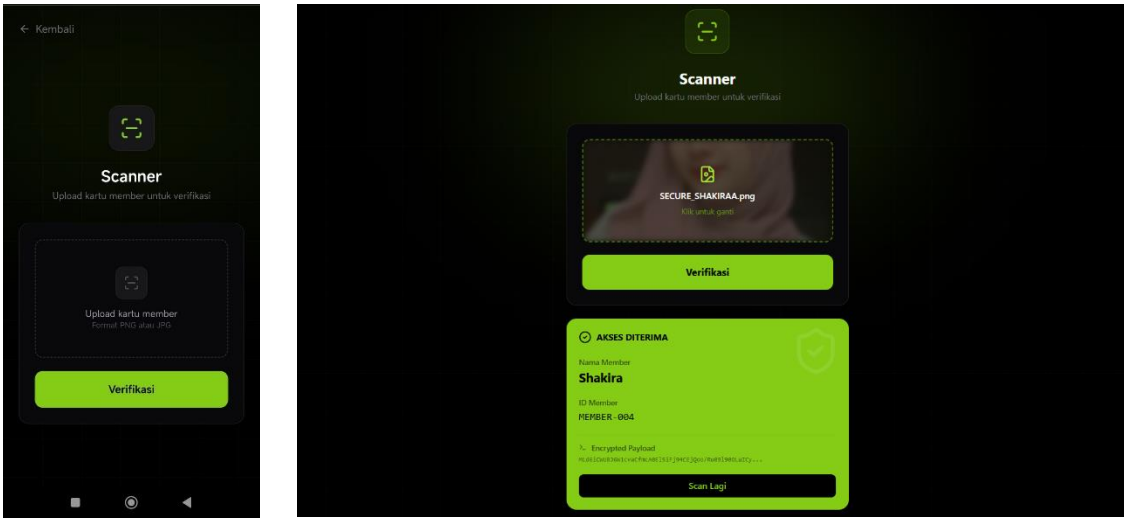
Kode Sample	Format Input	Dimensi (px)	Kedalaman Warna
Member_01	JPG	736x1308	24-bit (RGB)
Member_02	JPG	736x1308	24-bit (RGB)
Member_03	JPG	720x1249	24-bit (RGB)
Member_04	JPG	736x1308	24-bit (RGB)

Implementasi Antarmuka Sistem

Realisasi dari rancangan metode keamanan yang diusulkan diwujudkan dalam bentuk perangkat lunak berbasis web (*web service*) yang berfungsi sebagai generator token kehadiran. Sistem ini dikembangkan dengan memanfaatkan pustaka pemrosesan citra tingkat lanjut untuk menangani operasi matriks piksel secara presisi. Pada modul utama, sistem menerima masukan berupa nama lengkap, ID anggota, dan berkas foto profil, yang kemudian diproses melalui mekanisme keamanan hibrida. Penerapan arsitektur berbasis web ini dipilih untuk memfasilitasi integrasi sistem yang fleksibel dan efisien, sejalan dengan studi implementasi kriptografi modern yang menekankan pentingnya performa komputasi pada lingkungan jaringan [15]. Antarmuka sistem saat melakukan proses enkripsi data kredensial dan penyisipannya ke dalam citra profil ditampilkan pada Gambar 5 dan 6.



Gambar 5: Antarmuka Admin untuk memproses Stegano Image



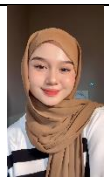
Gambar 6: Antarmuka user untuk melakukan Absensi (proses dekripsi)

Sistem secara otomatis mengelola alur kerja mulai dari validasi input, pembuatan *Initialization Vector* (IV) untuk AES-128, hingga konversi format citra akhir. Hasil dari proses ini adalah berkas citra steganografi yang secara fungsional siap digunakan sebagai token autentikasi. Keberhasilan implementasi antarmuka ini membuktikan bahwa kombinasi algoritma steganografi LSB dan kriptografi AES dapat diterapkan secara praktis dalam sebuah aplikasi keamanan data riil, tidak hanya sebatas simulasi teoritis.

Evaluasi Visual dan Analisis Ukuran File

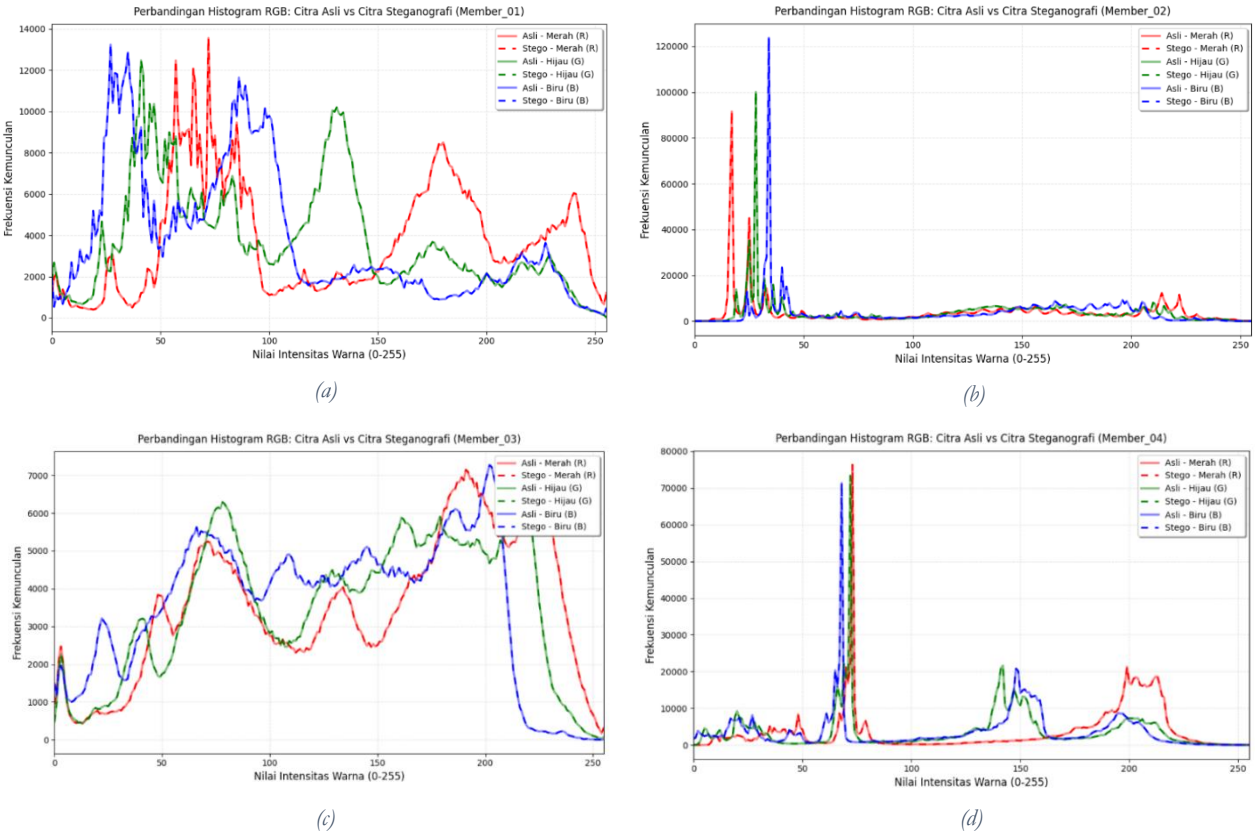
Pengujian visual dilakukan dengan membandingkan citra asli (*cover image*) dengan citra hasil steganografi (*stego image*) secara berdampingan. Berdasarkan pengamatan yang disajikan pada Tabel 2, tidak ditemukan adanya distorsi visual, artefak, atau perubahan kontras yang mencurigakan pada citra hasil. Citra steganografi terlihat identik dengan citra aslinya. Namun, dari segi ukuran file, terjadi peningkatan yang signifikan. Peningkatan ini merupakan konsekuensi logis dari dua faktor: pertama, perubahan format dari JPG (kompresi tinggi) menjadi PNG (tanpa kompresi data piksel), dan kedua, peningkatan entropi data akibat penyisipan *ciphertext* acak pada lapisan LSB yang sedikit mengurangi efisiensi kompresi PNG. Peningkatan ukuran ini masih dalam batas wajar untuk kebutuhan transmisi data dan dianggap sebagai *trade-off* yang diperlukan demi keamanan data.

Tabel 2: Spesifikasi Dataset Citra Uji dan Konversi Format

Sample	Member_01	Member_02	Member_03	Member_04
Citra Asli (JPG)				
Ukuran Awal	77,0 KB	76,8 KB	123 KB	72,6 KB
Citra Hasil (PNG)				
Ukuran Akhir	807 KB	667 KB	1,04 MB	531 KB
Kualitas Visual	Identik	Identik	Identik	Identik

Analisis Statistik Histogram

Validasi keamanan sistem tidak hanya terbatas pada aspek visual semata, melainkan juga harus mencakup ketahanan terhadap serangan statistik atau *steganalysis*. Dalam konteks keamanan jaringan, perubahan drastis pada distribusi frekuensi warna seringkali menjadi anomali yang memicu kecurigaan adanya manipulasi data oleh pihak ketiga. Oleh karena itu, analisis histogram menjadi instrumen validasi yang krusial untuk memastikan bahwa penyisipan bit LSB tidak mendistorsi profil statistik global citra, sehingga pesan tetap aman dari algoritma deteksi otomatis.



Gambar 7: Grafik Perbandingan Histogram RGB Citra Asli dan Stego-Image untuk keempat gambar

Analisis statistik pada Gambar 7 memperlihatkan grafik histogram gabungan (*overlay*) di mana garis grafik putus-putus dari citra steganografi menindih garis solid citra asli secara presisi pada ketiga kanal warna (Merah, Hijau, Biru). Keadaan garis yang saling berimpit ini membuktikan bahwa distribusi frekuensi intensitas warna tidak mengalami pergeseran signifikan pasca penyisipan data, mengonfirmasi bahwa teknik LSB yang diterapkan mampu menyembunyikan data rahasia tanpa merusak properti statistik citra sehingga sulit dideteksi baik secara visual maupun melalui analisis histogram sederhana.

Pengujian Kualitas Citra (MSE dan PSNR)

Evaluasi kuantitatif dilakukan untuk mengukur tingkat degradasi citra secara presisi menggunakan parameter *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR). Pengujian dilakukan terhadap empat sampel data dengan variasi ukuran piksel untuk menguji ketahanan metode terhadap beban muatan (*payload*) yang berbeda. Hasil pengukuran dirangkum secara rinci dalam Tabel 3.

Tabel 3: Hasil Pengujian Kualitas Citra (*Imperceptibility*)

Sampel Data (nama)	Panjang Payload(Bytes)	MSE	PSNR(RGB)	Kategori
Member_01 (Ani)	44	0.0001	89.72 dB	Sangat Baik
Member_02 (Anissa)	64	0.0001	88.53 dB	Sangat Baik
Member_03 (Putri)	44	0.0001	88.00 dB	Sangat Baik
Member_04 (Shakira)	64	0.0001	89.97 dB	Sangat Baik

Merujuk pada Tabel 3, nilai rata-rata PSNR yang diperoleh mencapai **89,05 dB**, jauh melampaui standar minimal kualitas citra yang baik yaitu 40 dB. Nilai MSE yang sangat rendah (rata-rata 0,0001) menunjukkan bahwa tingkat kesalahan atau perubahan piksel sangat minim. Hasil ini mengonfirmasi bahwa metode yang diusulkan memiliki tingkat *imperceptibility* yang sangat tinggi, di mana penambahan lapisan enkripsi AES tidak membebani kualitas visual citra secara signifikan.

Validasi Fungsionalitas Sistem

Tahap akhir pengujian adalah validasi fungsional untuk memastikan integritas data. Sistem diuji kemampuannya dalam mengekstraksi token dari *stego-image* dan mendekripsi *ciphertext* kembali menjadi teks asli (*plaintext*). Hasil pengujian pada Tabel 4 menunjukkan tingkat keberhasilan 100%.

Tabel 4: Hasil Pengujian Validasi Dekripsi dan Autentikasi

ID Sampel	Input Nama Asli	Status Enkripsi	Status Dekripsi	Kesesuaian Data
Member_01	Ani	Berhasil	Berhasil	Valid
Member_02	Anissa	Berhasil	Berhasil	Valid
Member_03	Putri	Berhasil	Berhasil	Valid
Member_04	Shakira	Berhasil	Berhasil	Valid

Mekanisme penanda batas (*delimiter*) yang diterapkan terbukti efektif membantu sistem memisahkan data payload dari *noise* piksel, sehingga proses dekripsi AES-CBC berjalan tanpa kesalahan *padding*. Dengan demikian, sistem ini dinyatakan layak dan aman untuk diterapkan sebagai metode autentikasi kehadiran.

Kesimpulan

Penelitian ini berhasil mengembangkan sistem autentikasi keamanan ganda untuk sistem kehadiran Gym DsFit dengan mengintegrasikan teknik kriptografi *Advanced Encryption Standard* (AES-128) dan steganografi *Least Significant Bit* (LSB). Berdasarkan hasil implementasi dan pengujian, sistem terbukti efektif menjawab permasalahan kerentanan manipulasi identitas pada metode presensi konvensional. Transformasi citra profil anggota menjadi token digital aktif telah divalidasi keberhasilannya melalui pengujian fungsional, di mana sistem mampu mengekstraksi dan mendekripsi data kredensial anggota dengan tingkat akurasi 100%. Dari aspek kualitas citra, metode yang diusulkan menunjukkan performa yang sangat baik dalam menyembunyikan data rahasia. Hal ini dibuktikan secara terukur dengan nilai rata-rata *Peak Signal-to-Noise Ratio* (PSNR) sebesar **89,05 dB** dan *Mean Square Error* (MSE) sebesar 0,0001, serta didukung oleh analisis histogram RGB yang menunjukkan grafik berimpit sempurna antara citra asli dan token steganografi. Temuan ini menegaskan bahwa mekanisme keamanan yang dibangun tidak hanya handal dalam melindungi kerahasiaan data, tetapi juga menjaga integritas visual citra sehingga sulit dideteksi oleh pihak ketiga. Untuk

pengembangan selanjutnya, disarankan agar sistem dapat dikembangkan ke platform seluler (*mobile application*) dengan menerapkan algoritma kompresi citra yang adaptif terhadap perubahan format media sosial, serta mengeksplorasi penggunaan algoritma kriptografi asimetris seperti RSA untuk meningkatkan keamanan pertukaran kunci.

Daftar Rujukan

[1] F. Baso, N. A. Rais, H. Hatima, dan P. A. A. Nur, "Steganografi Berbasis Kecerdasan Buatan untuk Mengatasi Ancaman Terbaru dalam Keamanan Data," *Jurnal MediaTIK: Jurnal Media Pendidikan Teknik Informatika dan Komputer*, vol. 7, no. 3, hlm. 145–149, Sep 2024, doi: https://doi.org/10.59562/mediatik.v7i3.5526.

[2] A. S. Fadel, R. D. Saputra, R. N. Putra, dan Y. Fatma, "Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," *Jurnal CoSciTech (Computer Science and Information Technology)*, vol. 5, no. 1, hlm. 36–41, Apr 2024, doi: 10.37859/coscitech.v5i1.6759.

[3] A. Purbaningrum, K. Silvi Amalia, dan I. A. Saputro, "Penerapan Metode Least Significant Bit (LSB) dalam Menyisipkan Pesan Rahasia pada Citra Digital: Sebuah Pendekatan Steganografi," dalam *SEMINAR NASIONAL AMIKOM SURAKARTA (SEMNASA) 2023*, Sukoharjo, Nov 2023, hlm. 176–183.

[4] M. N. Al Jum'ah dan Arifin, "Analisis Pengaruh Kompresi File Pada Media Sosial Terhadap Ketahanan Image Steganografi Pada Metode Least Significant Bit (LSB)," *Jurnal CyberSecurity dan Forensik Digital*, vol. 8, no. 1, hlm. 97–106, Nov 2025, doi: https://doi.org/10.14421/csecurity.2025.8.2.5310.

[5] M. O. Abdillah, O. A. Pane, dan F. R. A. Lubis, "Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)," *Jurnal Sains dan Teknologi (JSIT)*, vol. 3, no. 1, hlm. 40–46, Jan 2023, doi: 10.47233/jsit.v3i1.482.

[6] M. N. Al Jum'ah dan Sarimuddin, "Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," *Jurnal Informatika dan Rekayasa Perangkat Lunak*, vol. 6, hlm. 102–108, Mar 2024, doi: https://doi.org/10.36499/jinrpl.v6i1.10143.

[7] S. Amini, M. Hardjianto, dan D. Kusumaningsih, "Perbandingan Penggunaan Bit Steganografi Metode Least Significant Bit (LSB) M-Bit Pada Citra Digital," *Jurnal TICOM: Technology of Information and Communication*, vol. 13, no. 3, hlm. 129–134, Mei 2025, doi: https://doi.org/10.70309/ticom.v13i3.157.

[8] C. Nugroho dan Muslihudin, "Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode Least Significant Bit & Steghide," *JIS (Jurnal Ilmu Siber)*, vol. 1, hlm. 51–54, Mei 2022.

[9] A. Khuzaifi, Fausiah, dan I. Fitri, "Teknik Steganography untuk Menyisipkan Pesan pada Sebuah Citra Menggunakan Metode Least Significant Bit (LSB)," *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, vol. 6, no. 3, hlm. 2022, 2022, doi: https://doi.org/10.35870/JTIK.V6I3.461.

[10] S. R. Rahmatillah *dkk.*, "Steganografi: Keamanan Data Dengan Metode Least Significant Bit Menggunakan Python," *JURSISTEKNI (Jurnal Sistem Informasi dan Teknologi Informasi)*, vol. 6, no. 2, hlm. 439–447, Mei 2024, doi: https://doi.org/10.52005/jursistekni.v6i2.327.

[11] S. Oktavani, F. Rizky, dan I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *Jurnal Media Informatika (JUMIN)*, vol. 4, no. 2, hlm. 97–101, Jun 2023, doi: https://doi.org/10.55338/jumin.v4i2.435.

[12] M. B. Aryanto, M. Tahir, S. I. Devita, Z. N. Mustofa, Q. Ainiyah, dan S. Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer*, vol. 3, no. 1, hlm. 89–104, Mar 2023, [Daring]. Tersedia pada: http://journal.sinov.id/index.php/juisik/indexHalamanUTAMAJurnal:https://journal.sinov.id/index.php

[13] C. Umam, Muslih, dan D. Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," dalam *2 st Proceeding STEKOM*, 2022, hlm. 109–118.

[14] M. R. A. Y. Putra, B. P. Aryatama, N. C. David, G. Pamungkas, dan I. A. Saputro, "Implementasi Steganografi Untuk Keamanan Jaringan Teknik Tersembunyi Dalam Komunikasi Data," *Jurnal Riset Multidisiplin Edukasi*, vol. 2, no. 10, hlm. 956–963, Okt 2025, doi: https://doi.org/10.71282/jurmie.v2i10.1093.

[15] A. S. Aswandi, M. N. Sutoyo, dan A. Pradipta, "Analisis Performa Dan Keamanan Implementasi Kriptografi AES Untuk Penyandian Dokumen Berbasis WEB," *Jurnal Ilmu Komputer dan Teknik Informatika*, vol. 8, no. 1, hlm. 24–32, Feb 2025, doi: https://doi.org/10.36040/mnemonic.v8i1.12053.