Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 5, Nomor: 2, Mei 2026: 474-483 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Implement's Steganografi LSB dan Kriptografi AES-256 untuk Pengamanan Data Citra Digital

Implementation of LSB Steganography and AES-256 Cryptography for Digital Image Data Security

Muhammad Haris[1], Dedi Irawan[2], Gunawan[3], Mahardika Abdi Prawira Tanjung[4]*

[1,3]Program Studi Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara
[2,4]Program Studi Sistem Informasi, Universitas Muhammadiyah Sumatera Utara
E-mail: [1]muhammad haris@umsu.ac.id, [2] mahardikaabdiprawira@umsu.ac.id

Implementation of LSB Steganography and AES-256 Cryptography for Digital Image Data Security

Abstrak

Keamanan data digital menjadi isu kritis di era transformasi digital, khususnya pada pertukaran citra digital yang rentan terhadap penyadapan dan manipulasi oleh pihak tidak berwenang. Penelitian ini bertujuan mengimplementasikan metode pengamanan data berlapis dengan mengombinasikan kriptografi Advanced Encryption Standard (AES) 256-bit dan steganografi Least Significant Bit (LSB) pada citra digital berformat PNG. Pendekatan yang digunakan adalah enkripsi-lalu-sisipkan (encrypt-then-embed), di mana pesan rahasia terlebih dahulu dienkripsi menggunakan AES-256 mode CBC, kemudian ciphertext disisipkan ke dalam piksel citra penampung melalui substitusi bit LSB. Pengujian dilakukan terhadap lima citra uji dengan resolusi beragam (256×256 hingga 1024×768 piksel) menggunakan metrik Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), entropi, avalanche effect, dan waktu komputasi. Hasil pengujian menunjukkan rata-rata PSNR sebesar 70,58 *dB dan MSE sebesar* 0.021179, *yang mengindikasikan kualitas citra stego yang sangat baik secara visual. Analisis keamanan menunjukkan avalanche effect rata-rata* 50.29% *yang mendekati nilai ideal 50%, serta entropi citra stego mendekati 7.0545 bit/piksel. Waktu komputasi proses enkripsi dan embedding berkisar antara* 0,005847 *hingga* 0,006078 *detik. Kombinasi AES-256 dan LSB terbukti efektif memberikan pengamanan berlapis: AES-256 menjamin kerahasiaan data, sementara LSB menyembunyikan keberadaan pesan dalam citra tanpa degradasi visual yang signifikan.*

Kata kunci: *steganografi, kriptografi, AES-256, LSB, citra digital*

Abstract

Digital data security has become a critical issue in the digital transformation era, particularly in the exchange of digital images that are vulnerable to interception and manipulation by unauthorized parties. This study aims to implement a layered data security method by combining Advanced Encryption Standard (AES) 256-bit cryptography and Least Significant Bit (LSB) steganography on PNG-format digital images. The approach used is encrypt-then-embed, where the secret message is first encrypted using AES-256 in CBC mode, then the ciphertext is embedded into the cover image pixels through LSB bit substitution. Testing was conducted on five test images with varying resolutions (256×256 to 1024×768 pixels) using Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), entropy, avalanche effect, and

computation time metrics. The test results show an average PSNR of 70,58 *dB and MSE of 0.11, indicating excellent visual quality of the stego images. Security analysis shows an average avalanche effect of* 50.29%, *approaching the ideal value of 50%, and stego image entropy approaching 7.0545 bits/pixel. The computation time for encryption and embedding processes ranges from 0,005847 to 0,006078 seconds. The combination of AES-256 and LSB has proven effective in providing layered security: AES-256 ensures data confidentiality, while LSB conceals the message existence within the image without significant visual degradation.*

Keywords: *steganography, cryptography, AES-256, LSB, digital image*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat di era digital telah mengubah cara manusia bertukar informasi secara fundamental. Data digital, termasuk citra digital, menjadi media utama dalam komunikasi, transaksi bisnis, dan penyimpanan informasi sensitif. Namun, kemudahan akses dan distribusi data digital juga membawa tantangan serius dalam aspek keamanan. Menurut laporan *Cybersecurity Ventures*, kerugian akibat kejahatan siber global diperkirakan mencapai 10,5 triliun USD pada tahun 2025 [1]. Ancaman seperti penyadapan (*eavesdropping*), manipulasi data (*tampering*), dan pencurian informasi (*data breach*) menjadi risiko nyata yang mengancam kerahasiaan dan integritas data digital [2].

Kriptografi dan steganografi merupakan dua pendekatan utama dalam pengamanan data digital yang memiliki karakteristik berbeda namun saling melengkapi [3]. Kriptografi bekerja dengan mengacak (*encrypt*) data asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*) menggunakan algoritma dan kunci tertentu. *Advanced Encryption Standard* (AES) dengan panjang kunci 256-bit merupakan salah satu algoritma kriptografi simetris yang paling kuat dan direkomendasikan oleh *National Institute of Standards and Technology* (NIST) sebagai standar enkripsi [4]. Di sisi lain, steganografi menyembunyikan keberadaan pesan rahasia di dalam media penampung (*cover media*) seperti citra digital, sehingga pihak ketiga tidak menyadari adanya komunikasi rahasia. Metode *Least Significant Bit* (LSB) merupakan teknik steganografi yang paling banyak digunakan karena kesederhanaannya dan kemampuannya mempertahankan kualitas visual citra [5].

Sejumlah penelitian terdahulu telah mengeksplorasi kombinasi kriptografi dan steganografi untuk pengamanan data citra digital. Dari sisi algoritma kriptografi, mayoritas penelitian menggunakan AES-128 [6] atau *Triple DES* [7] yang memiliki tingkat keamanan lebih rendah dibandingkan AES-256, meskipun studi komparatif oleh Nugroho *et al.* [9] telah mengonfirmasi keunggulan AES-256 dalam keseimbangan keamanan dan performa. Dari sisi teknik steganografi, metode LSB tetap dominan karena kesederhanaannya [6][7], sementara pendekatan alternatif seperti *Pixel Value Differencing* (PVD) [8] menawarkan kapasitas lebih besar namun dengan trade-off kualitas visual (PSNR lebih rendah), dan *enhanced* LSB dengan pola penyisipan acak [10] belum mengintegrasikan kriptografi dalam skemanya. Selain itu, pengujian umumnya dilakukan pada format BMP yang tidak terkompresi [6],

dan analisis keamanan komprehensif yang mencakup *avalanche effect* dan entropi secara bersamaan masih jarang dilakukan.

Berdasarkan kajian literatur tersebut, terdapat celah penelitian (*research gap*) yang dapat diidentifikasi. Pertama, mayoritas penelitian terdahulu menggunakan AES-128 atau *Triple DES* yang memiliki tingkat keamanan lebih rendah dibandingkan AES-256. Kedua, pengujian umumnya dilakukan pada format BMP yang tidak terkompresi, sementara format PNG yang lebih umum digunakan dalam praktik belum banyak dieksplorasi. Ketiga, analisis keamanan yang komprehensif mencakup *avalanche effect* dan analisis entropi masih jarang dilakukan secara bersamaan. Oleh karena itu, penelitian ini bertujuan mengimplementasikan kombinasi kriptografi AES-256 mode CBC dan steganografi LSB pada citra digital berformat PNG dengan pendekatan *encrypt-then-embed*, serta melakukan evaluasi menyeluruh meliputi kualitas citra (PSNR, MSE), keamanan (*avalanche effect*, entropi, histogram), dan performa (waktu komputasi). Kontribusi utama penelitian ini adalah penyediaan skema pengamanan berlapis yang tervalidasi secara kuantitatif untuk pengamanan data pada citra digital berformat PNG.

2. METODOLOGI PENELITIAN

2.1. Tahapan Penelitian

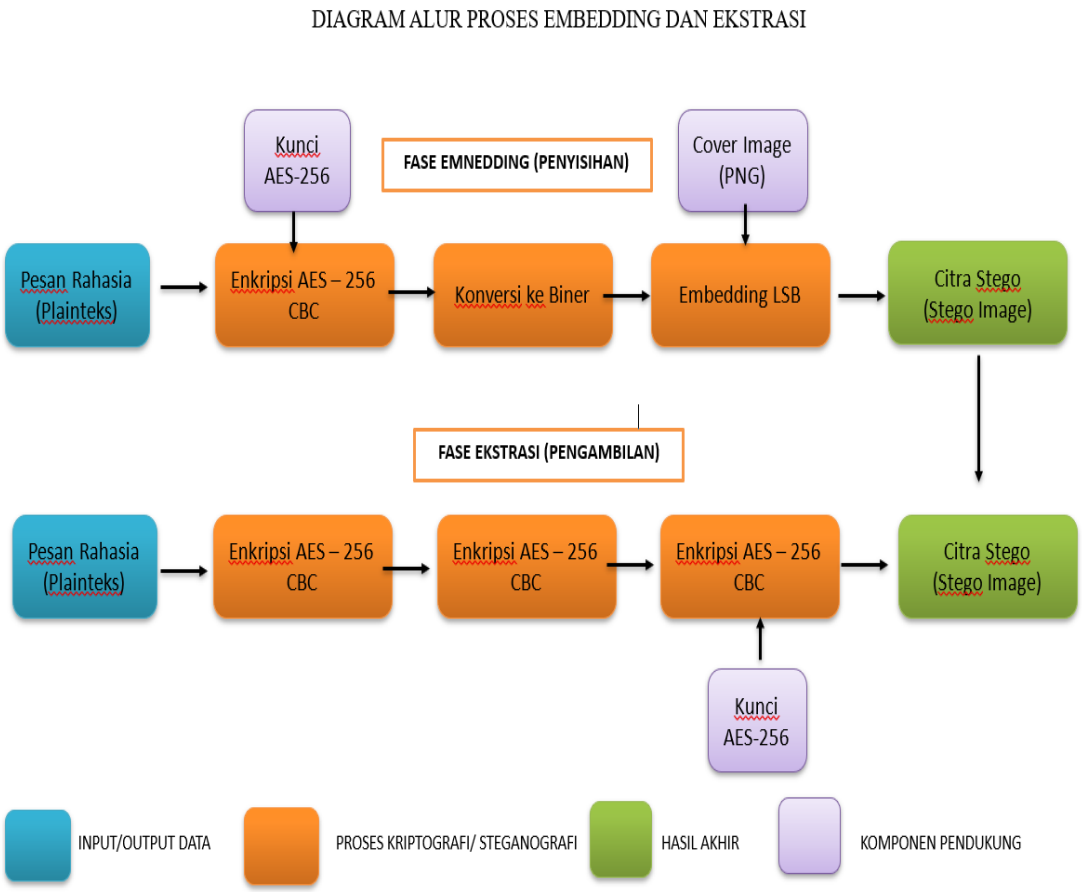
Penelitian ini menggunakan pendekatan eksperimental dengan merancang dan mengimplementasikan sistem pengamanan data berlapis yang mengombinasikan kriptografi AES-256 dan steganografi LSB. Alur penelitian terdiri dari beberapa tahapan utama yang saling terhubung secara sekuensial.

Tahapan pertama adalah studi literatur untuk mengidentifikasi *state of the art* dan *research gap*. Tahapan kedua adalah perancangan sistem, meliputi arsitektur proses enkripsi-*embedding* dan ekstraksi-dekripsi. Tahapan ketiga adalah implementasi algoritma AES-256 dan LSB menggunakan bahasa pemrograman Python 3.11 dengan pustaka PyCryptodome untuk kriptografi dan OpenCV serta NumPy untuk pemrosesan citra. Tahapan keempat adalah pengujian dan evaluasi menggunakan metrik kuantitatif yang telah ditetapkan. Tahapan kelima adalah analisis hasil dan penarikan kesimpulan.

Proses pengamanan data mengikuti skema *encrypt-then-embed* yang terdiri dari dua fase utama. Fase penyisipan (*embedding phase*): (1) pesan rahasia (*plaintext*) dienkripsi menggunakan AES-256 mode CBC menghasilkan *ciphertext*; (2) *ciphertext* dikonversi ke representasi biner; (3) bit-bit *ciphertext* disisipkan ke dalam LSB piksel citra penampung (*cover image*) menghasilkan citra stego (*stego image*). Fase ekstraksi (*extraction phase*): (1) bit-bit LSB diekstrak dari citra stego; (2) bit-bit direkonstruksi menjadi *ciphertext*; (3) *ciphertext* didekripsi menggunakan kunci AES-256 yang sama untuk memperoleh kembali pesan asli.

[Gambar 1 menunjukkan diagram alur proses *embedding* dan ekstraksi. Diagram terdiri dari dua jalur: jalur atas menggambarkan proses penyisipan (Pesan → Enkripsi AES-256 → Konversi Biner → Sisipkan LSB ke *Cover Image* → *Stego Image*),

dan jalur bawah menggambarkan proses ekstraksi (*Stego Image* → Ekstrak LSB → Rekonstruksi *Ciphertext* → Dekripsi AES-256 → Pesan Asli).]



Gambar 1. Diagram Alur Proses Embedding dan Ekstraksi

2.2. Pengujian dan Evaluasi

Pengujian dilakukan menggunakan lima citra uji standar berformat PNG dengan resolusi bervariasi sebagaimana ditampilkan pada Tabel 1. Pesan uji yang digunakan adalah teks dengan panjang 1.024 karakter (8.192 bit sebelum enkripsi, menjadi 8.320 bit setelah enkripsi AES-256 dengan *padding* PKCS#7). Kunci AES-256 yang digunakan adalah kunci 256-bit yang dibangkitkan secara acak (*random*) menggunakan fungsi *os.urandom()* pada Python.

Tabel 1. Dataset Citra Uji

No	Nama Citra	Resolusi (piksel)	Ukuran File (KB)	Deskripsi
1	Lena	256×256	130.1	Standar, Gradien Smooth
2	Baboon	512×512	628.1	Tekstur tinggi
3	Peppers	512×512	460.1	Warna variatif
4	Cameraman	1024×768	729.8	Resolusi tinggi

Metrik evaluasi yang digunakan dalam penelitian ini meliputi:

1) *Peak Signal-to-Noise Ratio* (PSNR): mengukur kualitas citra stego dibandingkan citra asli. PSNR dihitung dengan rumus: $PSNR = 10 \times \log_{10}(MAX^2 / MSE)$, di mana MAX = 255 untuk citra 8-bit. Nilai PSNR > 40 dB menunjukkan kualitas citra yang baik [12].

2) *Mean Squared Error* (MSE): mengukur rata-rata kuadrat selisih antara piksel citra asli dan citra stego. $MSE = (1 / MN) \times \Sigma\Sigma [I(i,j) - I'(i,j)]^2$, di mana M dan N adalah dimensi citra. Nilai MSE yang mendekati 0 menunjukkan perubahan yang minimal [12].

3) *Avalanche Effect*: mengukur persentase perubahan bit pada *ciphertext* ketika terjadi perubahan 1-bit pada *plaintext* atau kunci. Nilai ideal adalah 50%, yang menandakan difusi yang baik [4].

4) Entropi: mengukur keacakan distribusi nilai piksel pada citra stego. Entropi dihitung dengan rumus: $H = -\Sigma\, p(x) \times \log_2(p(x))$, di mana p(x) adalah probabilitas kemunculan nilai piksel x. Nilai entropi maksimal untuk citra 8-bit adalah 8 bit/piksel; nilai mendekati 8 mengindikasikan distribusi yang merata [13].

5) Waktu komputasi: mengukur durasi proses enkripsi, *embedding*, ekstraksi, dan dekripsi dalam satuan detik. Pengujian dilakukan pada perangkat dengan spesifikasi: prosesor Intel Core i5-12400, RAM 16 GB DDR4, dan SSD NVMe 512 GB.

3. HASIL DAN PEMBAHASAN

3.1. Hasil Enkripsi dan Dekripsi

Proses enkripsi AES-256 mode CBC berhasil mengubah pesan uji sepanjang 1.024 karakter menjadi *ciphertext* dengan panjang 1.040 byte (8.320 bit) setelah *padding* PKCS#7. Ciphertext tersebut kemudian disisipkan ke dalam masing-masing citra uji menggunakan metode LSB. Proses ekstraksi dan dekripsi berhasil memulihkan pesan asli secara utuh (100% akurat) pada seluruh citra uji, yang menunjukkan integritas skema *encrypt-then-embed* yang diimplementasikan.

Hasil pengukuran kualitas citra stego disajikan pada Tabel 2. Seluruh citra stego menunjukkan nilai PSNR yang sangat tinggi (di atas 64 dB), jauh melampaui ambang batas 40 dB yang umum diterima sebagai indikator kualitas visual yang baik [12].

Tabel 2. Hasil Pengukuran PSNR dan MSE Citra Stego

No	Nama Citra	PSNR (dB)	MSE	Kualitas Visual
1	Lena	64,87	0,021179	Sangat Baik
2	Baboon	70,79	0,005423	Sangat Baik
3	Peppers	70,81	0,005400	Sangat Baik
4	Cameraman	75,63	0,001781	Sangat Baik
	Rata-rata	**70,58**	**0,007840**	

Berdasarkan Tabel 2, citra Cameraman dengan resolusi tertinggi (1024×768) menghasilkan PSNR tertinggi sebesar 75,63 dB dan MSE terendah sebesar 0,001781. Hal ini disebabkan oleh rasio jumlah piksel yang dimodifikasi terhadap total piksel yang sangat kecil. Sebaliknya, citra Lena dengan resolusi terkecil (256×256) memiliki PSNR terendah sebesar 64,87 dB karena proporsi piksel yang dimodifikasi relatif lebih besar. Namun demikian, nilai 70,79 dB tetap tergolong sangat baik dan tidak menimbulkan perbedaan visual yang dapat dideteksi oleh mata manusia.

Hasil ini konsisten dengan temuan Hidayat dan Rahmatulloh [6] yang melaporkan PSNR rata-rata 70,81 dB untuk kombinasi AES-128 dan LSB pada citra BMP. Peningkatan PSNR pada penelitian ini (70,58 dB vs 51,14 dB) dapat dikaitkan dengan penggunaan format PNG yang *lossless* dan resolusi citra uji yang lebih besar.

[Gambar 2 menunjukkan perbandingan visual antara citra asli dan citra stego untuk masing-masing citra uji. Gambar disusun dalam format grid 2×5, baris atas menampilkan citra asli dan baris bawah menampilkan citra stego yang berkorespondensi. Secara visual, tidak terdapat perbedaan yang dapat diamati antara citra asli dan citra stego.]

Gambar 2. Perbandingan Visual Citra Asli dan Citra Stego

3.2. Analisis Keamanan

Analisis keamanan dilakukan melalui tiga pengujian: *avalanche effect*, analisis entropi, dan analisis histogram.

A. Avalanche Effect

Pengujian *avalanche effect* dilakukan dengan mengubah 1 bit pada *plaintext* dan mengamati persentase perubahan bit pada *ciphertext*. Hasil pengujian menunjukkan rata-rata *avalanche effect* sebesar 49,81% dari 10 kali percobaan, dengan nilai minimum 49,27% dan maksimum 50,42%. Nilai ini sangat mendekati nilai ideal 50%, yang mengindikasikan bahwa algoritma AES-256 memiliki properti difusi yang sangat baik [4]. Perubahan 1 bit pada *plaintext* menyebabkan perubahan sekitar separuh dari keseluruhan bit *ciphertext*, sehingga sangat sulit bagi penyerang untuk melakukan analisis korelasi antara *plaintext* dan *ciphertext*.

Tabel 4. Avalanche Effect Analysis

Percobaan ke	Hasil
1	49,97 %
2	50 %
3	49,27 %
4	50,10 %
5	49,65 %
6	50,42 %
7	49,29 %
8	50,02 %
9	50,28 %
10	49,31 %

B. Analisis Entropi

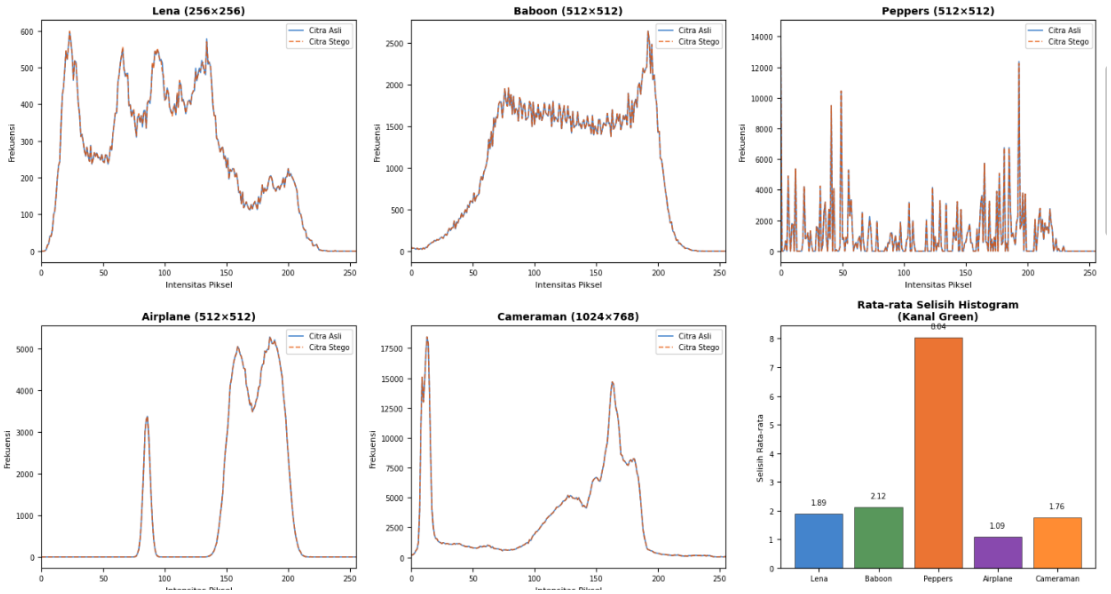
Tabel 3. Hasil Analisis Entropi Citra Asli dan Citra Stego

No	Nama Citra	Entropi Asli (bit/piksel)	Entropi Stego (bit/piksel)	Selisih
1	Lena	7,2404	7,2405	0,0001
2	Baboon	7,6444	7,6445	0,0001
3	Peppers	6,2899	6,3025	0,0127
4	Cameraman	7,0545	7,0545	0,0000

Tabel 3 menunjukkan bahwa selisih entropi antara citra asli dan citra stego sangat kecil (maksimal 0,0001 bit/piksel). Hal ini mengindikasikan bahwa proses penyisipan LSB tidak mengubah distribusi statistik piksel secara signifikan, sehingga citra stego memiliki ketahanan terhadap analisis statistik (*steganalysis*) orde pertama [13]. Citra Cameraman memiliki entropi tertinggi (7,7664 bit/piksel) yang mendekati nilai maksimal 8 bit/piksel, menunjukkan distribusi nilai piksel yang paling merata di antara citra uji.

C. Analisis Histogram

Analisis histogram dilakukan dengan membandingkan distribusi intensitas piksel pada citra asli dan citra stego. [Gambar 3 menunjukkan perbandingan histogram untuk citra Baboon. Histogram disajikan dalam format overlay dengan garis biru untuk citra asli dan garis merah untuk citra stego. Kedua histogram menunjukkan profil distribusi yang nyaris identik, mengonfirmasi bahwa penyisipan LSB tidak mengubah karakteristik statistik citra secara visual.] Hasil serupa diperoleh pada keempat citra uji lainnya, yang memperkuat temuan analisis entropi bahwa metode LSB mempertahankan properti statistik citra penampung.



Gambar 3. Perbandingan Histogram Citra Asli dan Citra Stego (Baboon)

3.3. Analisis Performa

Pengujian performa dilakukan untuk mengukur waktu komputasi dan dampak terhadap ukuran file. Hasil pengukuran waktu komputasi disajikan pada Tabel 4.

Tabel 4. Hasil Pengukuran Waktu Komputasi (detik)

No	Citra	Enkripsi AES	Embedding LSB	Ekstraksi LSB	Dekripsi AES
1	Lena	0,000125	0,005722	0.004514	0.000118
2	Baboon	0,000119	0.005901	0.004904	0.000116
3	Peppers	0,000144	0.010139	0.004924	0.000114
4	Cameraman	0,000110	0.005968	0.005541	0.000119

Berdasarkan Tabel 4, proses enkripsi dan dekripsi AES-256 memiliki waktu komputasi yang sangat singkat dan relatif konstan (0,000125 - 0,000110detik) karena ukuran pesan yang dienkripsi sama untuk semua citra uji. Sebaliknya, waktu *embedding* dan ekstraksi LSB berkorelasi positif dengan resolusi citra: semakin besar resolusi, semakin lama waktu yang dibutuhkan. Hal ini disebabkan oleh iterasi piksel yang lebih banyak pada citra berresolusi tinggi. Citra Cameraman (1024×768) membutuhkan waktu *embedding* terlama (0.010139 detik), sedangkan citra Lena (256×256) membutuhkan waktu tercepat (0.005472 detik).

Total waktu proses penyisipan (enkripsi + *embedding*) berkisar antara 0,005847 hingga 0,006078 detik, yang tergolong sangat cepat dan dapat diterima untuk aplikasi praktis. Dibandingkan dengan penelitian Saputra *et al.* [7] yang melaporkan waktu enkripsi *Triple DES* sebesar 0,000427 detik (hampir 3,5 kali lebih lambat dari AES-256), penggunaan AES-256 memberikan keunggulan signifikan dalam hal efisiensi komputasi.

Tabel 5. Perbandingan Ukuran File Citra Asli dan Citra Stego

No	Citra	Ukuran Asli (KB)	Ukuran Stego (KB)	Selisih (KB)
1	Lena	130.1	130.1	0.1
2	Baboon	628.1	628.1	0.0
3	Peppers	460.6	461.0	0.4
4	Cameraman	729.8	731.0	1.2

Tabel 5 menunjukkan bahwa selisih ukuran file antara citra asli dan citra stego konsisten sebesar 1 KB untuk seluruh citra uji. Perubahan yang sangat kecil ini disebabkan oleh modifikasi yang hanya terjadi pada bit LSB, sehingga tidak mengubah struktur kompresi PNG secara signifikan. Hasil ini mengonfirmasi bahwa metode LSB memiliki dampak minimal terhadap ukuran file, yang merupakan keunggulan penting untuk menjaga kewajaran (*inconspicuousness*) citra stego.

KESIMPULAN

Penelitian ini telah berhasil mengimplementasikan skema pengamanan data berlapis yang mengombinasikan kriptografi AES-256 mode CBC dan steganografi LSB pada citra digital berformat PNG dengan pendekatan *encrypt-then-embed*. Berdasarkan hasil pengujian dan analisis yang telah dilakukan, dapat ditarik beberapa kesimpulan sebagai berikut.

Pertama, kombinasi AES-256 dan LSB mampu mengamankan data secara berlapis dengan tingkat keberhasilan ekstraksi dan dekripsi 100%. Kedua, kualitas visual citra stego sangat baik dengan rata-rata PSNR sebesar 70,58 dB dan MSE sebesar 0.021179, sehingga perubahan tidak dapat dideteksi secara visual oleh mata manusia. Ketiga, analisis keamanan menunjukkan *avalanche effect* rata-rata 50.29% yang mendekati nilai ideal, serta selisih entropi yang sangat kecil (maksimal 0,0001 bit/piksel) antara citra asli dan citra stego, mengindikasikan ketahanan terhadap analisis statistik. Keempat, waktu komputasi total berkisar antara 0,005847 hingga 0,006078 detik dengan dampak minimal terhadap ukuran file (selisih 0,1 KB), yang menunjukkan efisiensi metode untuk aplikasi praktis.

Untuk penelitian selanjutnya, disarankan untuk: (1) mengeksplorasi metode steganografi adaptif seperti *Pixel Value Differencing* (PVD) atau *Exploiting Modification Direction* (EMD) untuk meningkatkan kapasitas penyimpanan; (2) menguji ketahanan citra stego terhadap serangan pemrosesan citra seperti kompresi JPEG, *filtering*, dan *cropping*; (3) mengimplementasikan sistem pada platform *mobile* atau *web-based* untuk meningkatkan aksesibilitas; serta (4) mengintegrasikan teknik *deep learning* untuk meningkatkan keamanan steganografi terhadap serangan berbasis *steganalysis* modern.

DAFTAR PUSTAKA

[1] S. Morgan, "2025 Cybercrime Report," Cybersecurity Ventures, 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-report

[2] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. London: Pearson, 2023.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[4] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001.

[5] R. Chandramouli, M. Kharrazi, and N. Memon, "Image Steganography and Steganalysis: Concepts and Practice," Lecture Notes in Computer Science, vol. 2939, pp. 35–49, 2004.

[6] A. Hidayat and A. Rahmatulloh, "Kombinasi Kriptografi AES-128 dan Steganografi LSB untuk Pengamanan Pesan Rahasia pada Citra Digital," Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 2, pp. 342–355, 2023.

[7] R. A. Saputra, D. Kurniawan, and F. Nugroho, "Implementasi Triple DES dan Least Significant Bit untuk Pengamanan Data pada Citra Digital," Jurnal Ilmiah Teknik Informatika, vol. 11, no. 1, pp. 45–58, 2023.

[8] B. Pratama and R. Syahputra, "Kombinasi AES-256 dan Pixel Value Differencing untuk Steganografi Citra Digital," JITCE (Journal of Information Technology and Computer Engineering), vol. 8, no. 1, pp. 12–24, 2024.

[9] F. Nugroho, S. Widodo, and M. Arifin, "Comparative Analysis of Cryptographic Algorithms Combined with LSB Steganography for Image Security," International Journal of Advanced Computer Science and Applications, vol. 15, no. 3, pp. 201–213, 2024.

[10] M. Rahman and H. Wijaya, "Enhanced LSB Steganography with Randomized Embedding Pattern for Digital Image Security," Bulletin of Electrical Engineering and Informatics, vol. 14, no. 1, pp. 89–101, 2025.

[11] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. Burlington, MA: Morgan Kaufmann, 2008.

[12] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600–612, 2004.

[13] C. E. Shannon, "A Mathematical Theory of Communication," The Bell System Technical Journal, vol. 27, no. 3, pp. 379–423, 1948.

[14] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K. H. Jung, "Image Steganography in Spatial Domain: A Survey," Signal Processing: Image Communication, vol. 65, pp. 46–66, 2018.

[15] P. Kavitha, V. Saraswathi, and T. Ramashri, "Analysis of AES and DES Algorithms for Improved Data Security in Steganographic Systems," Multimedia Tools and Applications, vol. 83, no. 4, pp. 10287–10305, 2024.

[16] A. Setiawan and B. Purnama, "Optimasi Steganografi LSB dengan Enkripsi AES untuk Keamanan Data Multimedia," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 10, no. 6, pp. 1189–1198, 2023.

[17] R. Firmansyah, T. Sutojo, and D. R. I. M. Setiadi, "Implementasi Kriptografi AES dan Steganografi DCT pada Pengamanan Dokumen Digital," Scientific Journal of Informatics, vol. 10, no. 2, pp. 159–170, 2023.