JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Implementasi Metode Least Significant Bit dan Advanced Encryption Standard pada Aplikasi Steganografi Berbasis Web

Nazrivan Ibrahim Siregar[1*], Bayu Samudera[2], Romi Okto Rifansah Panggabean[3], Ibnu Fauzan[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]nazrivan.230170124@unimal.ac.id, [2]bayu.230170116@unimal.ac.id, [3]romi.230170099@unimal.ac.id,
[4]ibnu.230170193@mhs.unimal.ac.id

ABSTRACT

Information security is a crucial aspect in the digital era, particularly in data transmission over the internet. In addition to cryptography, steganography serves as an alternative approach that conceals the existence of information itself. This study aims to design and implement a web-based digital steganography application by integrating the Least Significant Bit (LSB) method with the Advanced Encryption Standard (AES) algorithm. The LSB method is used to embed data into digital images by modifying the least significant bits, while AES encrypts the payload prior to embedding. The application is developed using PHP and a web-based interface. The results indicate that the system can embed text messages and document files into digital images without significantly affecting visual quality, and the hidden data can only be extracted using the correct password. Therefore, the integration of steganography and cryptography provides a dual-layer security mechanism for protecting digital information.

Keywords: *Steganography, Least Significant Bit, AES, Information Security, Web Application*

PENDAHULUAN

Perkembangan teknologi informasi berbasis jaringan telah mendorong peningkatan intensitas pertukaran data secara digital, khususnya melalui media internet dan aplikasi berbasis web. Kondisi tersebut secara tidak langsung juga meningkatkan potensi terjadinya kebocoran data dan penyalahgunaan informasi, terutama pada data yang bersifat rahasia dan sensitif. Oleh karena itu, aspek keamanan informasi menjadi kebutuhan penting dalam pengelolaan dan pertukaran data digital (Unik & Mukhtar, 2020).

Upaya pengamanan data umumnya dilakukan menggunakan teknik kriptografi, yaitu dengan mengubah data asli menjadi bentuk terenkripsi agar tidak dapat dipahami oleh pihak yang tidak berwenang. Namun demikian, data yang telah terenkripsi masih dapat menimbulkan kecurigaan karena keberadaannya terlihat secara langsung, baik pada media penyimpanan maupun saat proses transmisi berlangsung (Anwar et al., 2017).

Sebagai alternatif, steganografi hadir sebagai teknik pengamanan data yang berfokus pada penyembunyian keberadaan pesan itu sendiri. Pada steganografi digital, pesan rahasia disisipkan ke dalam media lain, seperti citra digital, sehingga keberadaannya sulit terdeteksi. Salah satu metode steganografi yang paling banyak digunakan adalah Least Significant Bit (LSB), yang memanfaatkan bit paling tidak signifikan pada nilai piksel citra. Perubahan pada bit tersebut umumnya tidak menimbulkan perbedaan visual yang berarti (Halim, 2023).

Untuk meningkatkan tingkat keamanan, teknik steganografi dapat dikombinasikan dengan kriptografi. Algoritma Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang banyak digunakan karena memiliki tingkat keamanan tinggi dan efisiensi yang baik. Integrasi steganografi dan kriptografi memberikan perlindungan ganda, yaitu menyembunyikan keberadaan data sekaligus mengamankan isi data tersebut (Firdaus et al., 2025). Oleh karena itu, penelitian ini mengusulkan pengembangan aplikasi steganografi digital berbasis web yang mengintegrasikan metode LSB dan algoritma AES sebagai solusi keamanan informasi yang lebih komprehensif.

TINJAUAN PUSTAKA

Steganografi Digital

Steganografi digital merupakan teknik penyembunyian informasi dengan cara menyisipkan pesan rahasia ke dalam media penampung (cover media) sehingga keberadaan pesan tersebut tidak mudah dikenali. Media yang sering digunakan dalam steganografi digital antara lain citra, audio, dan video. Tujuan utama steganografi tidak hanya menjaga kerahasiaan isi pesan, tetapi juga menyamarkan keberadaan pesan tersebut agar tidak menimbulkan kecurigaan (Halim, 2023).

Metode Least Significant Bit (LSB)

Metode Least Significant Bit (LSB) merupakan teknik steganografi yang bekerja dengan memodifikasi bit paling rendah dari nilai piksel citra digital untuk menyimpan data rahasia. Metode ini banyak digunakan karena implementasinya sederhana serta memiliki kapasitas penyisipan yang cukup baik. Perubahan pada bit LSB umumnya

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

tidak memengaruhi kualitas visual citra secara signifikan, sehingga sulit dibedakan oleh penglihatan manusia (Eka et al., 2025).

Kriptografi dan Algoritma Advanced Encryption Standard (AES)

Kriptografi merupakan teknik pengamanan data dengan cara mengubah informasi asli menjadi bentuk terenkripsi. Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris yang banyak digunakan dalam berbagai sistem keamanan data karena memiliki tingkat keamanan tinggi dan efisiensi komputasi yang baik. Penggunaan AES dalam steganografi bertujuan untuk memastikan bahwa data tetap terlindungi meskipun berhasil diekstraksi dari media penampung (Firdaus et al., 2025).

Penelitian Terkait

Beberapa penelitian sebelumnya telah membahas penerapan steganografi menggunakan metode LSB serta integrasinya dengan algoritma AES. Penelitian oleh Unik & Mukhtar (2020) menunjukkan bahwa kombinasi LSB dan AES mampu meningkatkan keamanan data secara signifikan. Penelitian lain oleh Anwar et al., (2017) juga menegaskan bahwa steganografi LSB efektif digunakan untuk pengamanan pesan teks pada citra digital. Namun, sebagian besar penelitian tersebut belum secara khusus mengimplementasikan sistem dalam bentuk aplikasi berbasis web yang mendukung penyisipan multi-payload. Oleh karena itu, penelitian ini difokuskan pada pengembangan aplikasi steganografi berbasis web yang lebih fleksibel dan mudah digunakan.

METODE PENELITIAN

Berdasarkan kajian pustaka dan penelitian terkait yang telah dibahas pada bagian sebelumnya, penelitian ini dilanjutkan dengan penyusunan metodologi penelitian. Metodologi penelitian ini digunakan sebagai panduan sistematis dalam merancang, mengimplementasikan, serta menguji aplikasi steganografi digital berbasis web yang dikembangkan, sehingga tujuan penelitian dapat tercapai secara terukur dan terstruktur. Metodologi penelitian yang digunakan dalam pengembangan aplikasi ini terdiri dari beberapa tahapan, yaitu analisis kebutuhan, perancangan sistem, implementasi, dan pengujian.

Arsitektur Sistem

Sistem dikembangkan dalam bentuk aplikasi web dengan arsitektur client-server. Pengguna mengakses sistem melalui browser untuk melakukan proses login, encode, dan decode. Proses pengolahan citra, enkripsi, serta ekstraksi data dilakukan pada sisi server.

Algoritma Least Significant Bit (LSB)

Metode LSB digunakan untuk menyisipkan data rahasia ke dalam citra digital dengan cara mengganti bit paling tidak signifikan pada nilai piksel citra. Metode ini dipilih karena implementasinya sederhana dan tidak menimbulkan perubahan visual yang signifikan pada citra hasil penyisipan.

Algoritma Advanced Encryption Standard (AES)

Algoritma AES digunakan untuk mengenkripsi payload berupa pesan teks atau dokumen sebelum proses penyisipan ke dalam citra. Proses enkripsi dilakukan menggunakan kata sandi yang ditentukan oleh pengguna, sehingga data yang berhasil diekstraksi tetap tidak dapat dibaca tanpa kunci yang sesuai.

Integrasi LSB dan AES

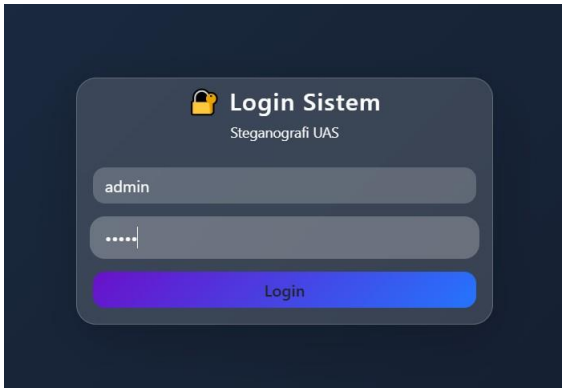
Integrasi dilakukan dengan mengenkripsi payload menggunakan AES, kemudian hasil enkripsi dikonversi ke dalam bentuk biner dan disisipkan ke dalam citra menggunakan metode LSB. Proses decode dilakukan dengan mengekstraksi data dari citra stego dan mendekripsinya kembali menggunakan kunci AES yang sama.

HASIL DAN PEMBAHASAN

Implementasi Sistem

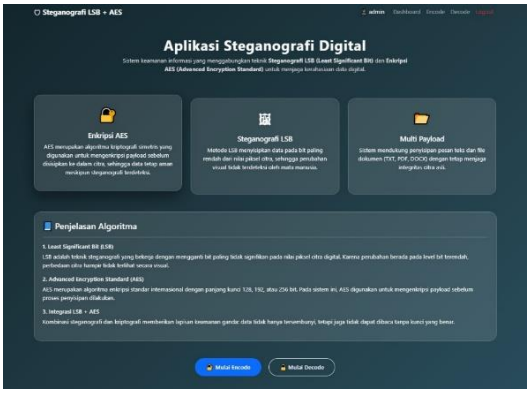
Aplikasi steganografi digital diimplementasikan sebagai aplikasi web berbasis client-server. Sistem menyediakan fitur login pengguna, dashboard utama, halaman encode untuk penyisipan data, serta halaman decode untuk ekstraksi pesan atau dokumen. Implementasi berbasis web dipilih untuk memudahkan akses tanpa memerlukan instalasi tambahan pada sisi pengguna.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026



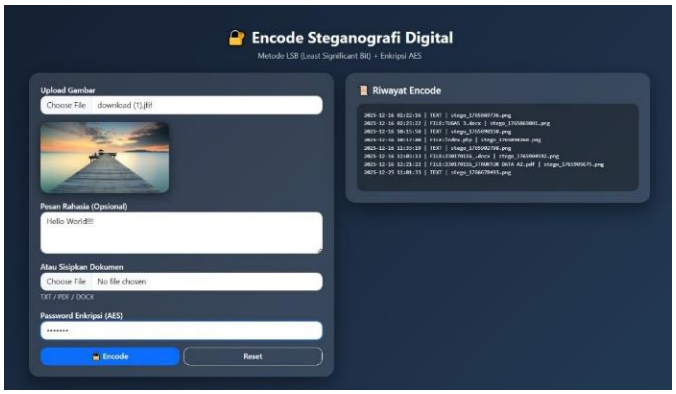
Gambar 1. Antarmuka Login Sistem

Gambar 1 menunjukkan halaman login yang digunakan sebagai mekanisme autentikasi pengguna sebelum mengakses fitur utama sistem. Fitur ini bertujuan untuk mencegah akses tidak sah terhadap fungsi encode dan decode.



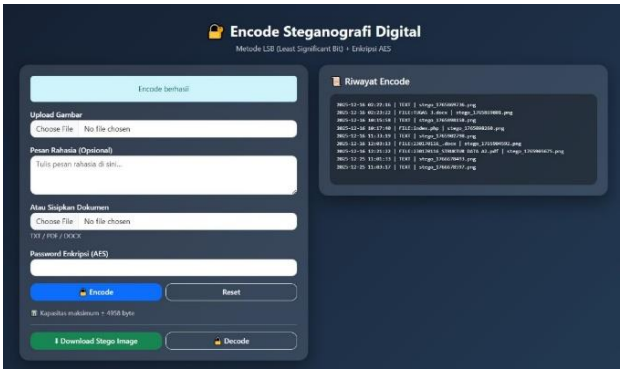
Gambar 2. Dashboard Aplikasi

Gambar 2 memperlihatkan dashboard utama sistem yang berfungsi sebagai pusat navigasi dan informasi. Dashboard memudahkan pengguna untuk mengakses fitur encode, decode, serta memantau riwayat proses penyisipan data.



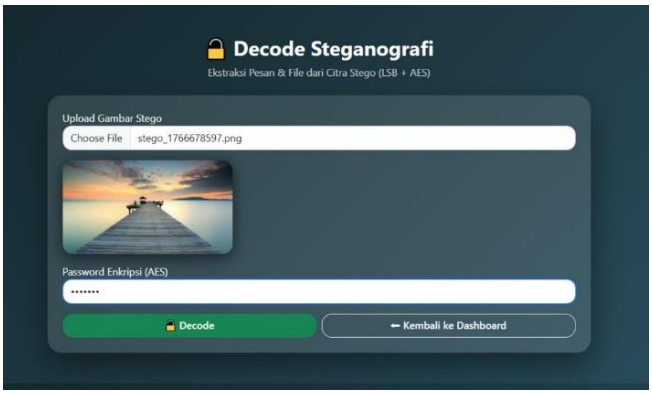
Gambar 3. Halaman Encode Steganografi Digital

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026



Gambar 4. Halaman Encode Steganografi Digital

Gambar 3 dan 4 menampilkan antarmuka proses encode, di mana pengguna dapat mengunggah citra digital, memasukkan pesan teks atau dokumen, serta menentukan kata sandi enkripsi AES sebelum data disisipkan menggunakan metode LSB.



Gambar 5. Halaman Decode Steganografi

Gambar 6. Halaman Decode Steganografi

Gambar 5 dan 6 menunjukkan halaman decode yang digunakan untuk mengekstraksi pesan atau dokumen tersembunyi dari citra stego. Proses dekripsi hanya dapat dilakukan dengan memasukkan kata sandi AES yang sesuai.

Pengujian Fungsional

Pengujian sistem dilakukan menggunakan metode black-box testing untuk memastikan seluruh fungsi berjalan sesuai dengan kebutuhan. Hasil pengujian menunjukkan bahwa sistem mampu menyisipkan dan mengekstraksi pesan teks maupun dokumen dengan baik, selama kapasitas citra mencukupi dan kata sandi yang digunakan sesuai.

Analisis Keamanan

Kombinasi steganografi dan kriptografi memberikan tingkat keamanan yang lebih tinggi dibandingkan penggunaan salah satu teknik secara terpisah. Data tidak hanya disembunyikan di dalam citra, tetapi juga dilindungi oleh enkripsi AES. Dengan demikian, meskipun citra stego berhasil diperoleh oleh pihak yang tidak berwenang, isi

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

pesan tetap tidak dapat dibaca tanpa kunci yang sesuai.

Pengujian Sistem (Black-Box Testing)

Pengujian sistem dilakukan menggunakan metode black-box testing, yaitu pengujian yang berfokus pada kesesuaian keluaran sistem terhadap masukan yang diberikan tanpa melihat struktur internal kode program. Pengujian ini bertujuan untuk memastikan seluruh fungsi utama aplikasi berjalan sesuai dengan kebutuhan pengguna.

Tabel 1. Hasil Pengujian Fungsional Sistem (Black-Box Testing)

No	Skenario Pengujian	Data Uji	Hasil yang Diharapkan	Hasil Pengujian
1	Login pengguna	Username dan password valid	Pengguna berhasil masuk ke sistem	Berhasil
2	Login pengguna	Username atau password tidak valid	Sistem menolak akses dan menampilkan pesan kesalahan	Berhasil
3	Encode pesan teks	Gambar valid, pesan teks, password	Data berhasil disisipkan ke dalam citra	Berhasil
4	Encode dokumen	Gambar valid, file dokumen, password	Dokumen berhasil disisipkan ke dalam citra	Berhasil
5	Decode data	Citra stego dan password benar	Pesan atau dokumen berhasil diekstraksi	Berhasil
6	Decode data	Citra stego dan password salah	Data tidak dapat diekstraksi	Berhasil

Berdasarkan hasil pengujian pada Tabel 1, dapat disimpulkan bahwa seluruh fungsi utama sistem telah berjalan sesuai dengan spesifikasi yang dirancang. Sistem mampu menangani berbagai kondisi masukan dan memberikan keluaran yang tepat sesuai dengan skenario pengujian.

KESIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan bahwa aplikasi steganografi digital berbasis web dengan metode Least Significant Bit (LSB) dan enkripsi Advanced Encryption Standard (AES) berhasil dikembangkan dan berfungsi sesuai dengan tujuan penelitian. Sistem mampu menyisipkan serta mengekstraksi pesan teks dan dokumen ke dalam citra digital tanpa menurunkan kualitas visual secara signifikan.

Integrasi metode LSB dan algoritma AES memberikan lapisan keamanan ganda, di mana data tidak hanya disembunyikan keberadaannya tetapi juga dilindungi melalui proses enkripsi. Dengan demikian, aplikasi ini efektif digunakan sebagai solusi keamanan informasi berbasis web.

Penelitian ini masih memiliki keterbatasan, antara lain sistem hanya diuji pada jenis citra tertentu dan belum dilakukan pengujian ketahanan terhadap teknik steganalisis lanjutan. Penelitian selanjutnya dapat mengembangkan sistem dengan metode steganografi lain serta menambahkan analisis kualitas citra secara kuantitatif.

REFERENSI

Anwar, S., Komputer, M. I., & Luhur, U. B. (2017). *IMPLEMENTASI PENGAMANAN DATA DAN INFORMASI DENGAN*. 37–42.

Eka, G., Wijaya, P., Agung, I. G., & Arya, G. (2025). *Penerapan Steganografi untuk Pengamanan Konten Gambar dalam Media Sosial*. *3*, 337–342.

Firdaus, M. A., Rahmatulloh, A., Teknik, F., & Siliwangi, U. (2025). *IMPLEMENTASI STEGANOGRAFI CITRA DIGITAL LSB MENGGUNAKAN ENKRIPSI AES-256 DAN EMBEDDING*. *13*(1).

Halim, M. (2023). *JURNAL ARMADA INFORMATIKA Steganography Menggunakan Advanced Encryption Standard dan Metode Least Significant Bit pada File Bitmap 24-bit*.

Unik, M., & Mukhtar, H. (2020). *Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)*. *1*(1), 8–12.

{