JIKUM
JURNAL ILMU KOMPUTER

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

Rancang Bangun Aplikasi Steganografi Berbasis Web Menggunakan Metode Least Significant Bit (LSB) Dan XOR Untuk Enkripsi File Berbasis Citra

Indra Firmansyah[1], Bayu Winata[2], Diana Azkia [3], Rahmatul Ula [4]
[1,2,3,4] Universitas Malikussaleh, Indonesia
[1] indra.220170088@unimal.ac.id, [2] bayu.220170103@unimal.ac.id, [3]diana.230170121@unimal.ac.id,
[4]rahmatul.230170108@unimal.ac.id

ABSTRACT

Data security is vital in digital exchange, yet standard Least Significant Bit (LSB) steganography remains vulnerable to unauthorized extraction. This study aims to develop a web-based steganography application combining LSB with Exclusive OR (XOR) encryption to enhance confidentiality. The proposed method involves encrypting secret data using XOR operations before embedding it into the cover image's LSB. The application is built on a web platform for accessibility, and the resulting image quality is evaluated using Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The results demonstrate that the system successfully embeds and extracts data intactly. The obtained PSNR values exceed 40 dB, indicating that the stego-images maintain high visual fidelity indistinguishable from the original images, thereby offering a robust solution for secure data transmission.

Keywords: *Steganography, LSB, XOR, Web Application, Data Security.*

PENDAHULUAN

Perkembangan teknologi informasi dan internet saat ini telah memfasilitasi pertukaran data digital secara cepat dan masif. Namun, kemudahan ini juga membawa risiko keamanan yang serius, seperti penyadapan, pencurian data, dan manipulasi informasi oleh pihak yang tidak berwenang. Oleh karena itu, aspek keamanan dan kerahasiaan data (*confidentiality*) menjadi prioritas utama dalam komunikasi digital. Untuk menjaga keamanan pesan, terdapat dua teknik utama yang sering digunakan, yaitu kriptografi dan steganografi. Kriptografi mengamankan pesan dengan cara menjadikannya bentuk yang tidak dapat dibaca, sedangkan steganografi bekerja dengan cara menyembunyikan keberadaan pesan itu sendiri ke dalam media penampung (*cover object*) sehingga tidak menimbulkan kecurigaan.

Salah satu media yang populer digunakan dalam steganografi adalah citra digital, dikarenakan citra memiliki redundansi data yang cukup besar yang dapat dimanfaatkan untuk menyisipkan pesan. Metode yang paling umum dan sederhana dalam steganografi citra adalah *Least Significant Bit* (LSB). Metode ini bekerja dengan mengganti bit paling tidak signifikan dari setiap piksel citra dengan bit pesan rahasia. Keunggulan metode LSB terletak pada kapasitas penyisipan yang besar dan kemudahannya dalam implementasi. Secara visual, perubahan pada bit terakhir ini tidak memberikan perbedaan yang signifikan pada citra hasil (*stego-image*) dibandingkan dengan citra aslinya.

Meskipun metode LSB memiliki kelebihan dari segi kapasitas dan kualitas visual, metode ini memiliki kelemahan mendasar dari sisi keamanan. Pesan yang disisipkan menggunakan LSB murni tanpa enkripsi sangat rentan untuk diekstrak oleh pihak ketiga. Jika penyerang mengetahui bahwa sebuah citra mengandung pesan rahasia dan mengetahui algoritma LSB yang digunakan, pesan tersebut dapat dipulihkan dengan mudah karena tersimpan dalam bentuk *plaintext*. Oleh karena itu, penggunaan steganografi LSB saja tidak lagi dianggap cukup aman untuk mentransmisikan data yang bersifat sangat rahasia.

Untuk mengatasi kelemahan tersebut, diperlukan lapisan keamanan tambahan berupa enkripsi data sebelum proses penyisipan dilakukan. Salah satu algoritma enkripsi yang efisien dan cepat adalah *Exclusive OR* (XOR). Algoritma XOR memiliki karakteristik sederhana namun efektif, di mana data yang dienkripsi dapat dikembalikan ke bentuk semula menggunakan kunci yang sama tanpa memerlukan komputasi yang berat, sehingga sangat cocok diimplementasikan pada aplikasi berbasis web yang membutuhkan respons cepat. Kombinasi antara kriptografi (XOR) dan steganografi (LSB) diharapkan dapat menciptakan sistem keamanan ganda (*double layer security*); jika steganografi terdeteksi, penyerang masih harus memecahkan enkripsi untuk membaca pesan.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang dan membangun sebuah aplikasi steganografi berbasis web menggunakan metode LSB dan enkripsi XOR. Pemilihan *platform* berbasis web ditujukan untuk memberikan fleksibilitas dan kemudahan akses bagi pengguna tanpa perlu melakukan instalasi perangkat lunak khusus. Penelitian ini juga akan mengukur kualitas citra hasil steganografi menggunakan parameter *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) untuk memastikan bahwa penambahan fitur enkripsi tidak merusak kualitas visual citra penampung secara signifikan.

JIKUM
JURNAL ILMU KOMPUTER

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

TINJAUAN PUSTAKA

Steganografi dan Citra Digital

Steganografi adalah seni dan ilmu menyembunyikan informasi dengan cara menyisipkan pesan ke dalam media pembawa (*cover object*) sedemikian rupa sehingga keberadaan pesan tersebut tidak diketahui oleh orang lain selain pengirim dan penerima yang dituju (Rohmanu, 2017). Berbeda dengan kriptografi yang menyamarkan makna pesan, steganografi menyamarkan keberadaan pesan itu sendiri. Media digital yang paling umum digunakan sebagai penampung adalah citra digital (*digital image*) (Nirmala et al., 2023). Citra digital merupakan representasi visual yang tersusun atas sekumpulan piksel, di mana setiap piksel memiliki nilai intensitas warna tertentu. Struktur data citra yang besar dan memiliki redundansi (data berlebih) memungkinkan penyisipan data asing tanpa merusak persepsi visual manusia secara signifikan (Nandar Pabokory et al., 2015).

Steganografi Metode *Least Significant Bit* (LSB)

Metode *Least Significant Bit* (LSB) merupakan teknik steganografi pada domain spasial yang paling populer karena kesederhanaan dan kapasitas penyimpanannya yang besar (Ryan Kuncoro & Aditama, 2019). Prinsip kerja LSB adalah mengganti bit paling tidak signifikan (bit ke-8 atau paling kanan) dari setiap byte data piksel pada citra penampung dengan bit data pesan rahasia. Pada citra 24-bit (RGB), setiap piksel terdiri dari 3 komponen warna (Merah, Hijau, Biru), yang berarti satu piksel dapat menampung 3 bit data rahasia (Parhusip & Sari, 2024).

Secara teoritis, perubahan pada LSB hanya mengubah nilai intensitas warna sebesar +/- 1 unit. Perubahan sekecil ini tidak dapat dideteksi oleh mata manusia (*Human Visual System*), sehingga citra hasil (*stego-image*) tampak identik dengan citra asli (Maria Baria Set et al., 2022). Namun, kelemahan utama metode ini adalah rendahnya tingkat keamanan terhadap serangan statistik atau *steganalysis*. Jika pola penyisipan diketahui, pesan dapat diekstrak dengan mudah tanpa memerlukan kunci khusus (Na & Al Jum, 2025).

Algoritma Kriptografi Exclusive OR (XOR)

Algoritma ini digunakan untuk menutupi kelemahan keamanan pada LSB, diterapkan teknik kriptografi sebelum proses penyisipan. Algoritma *Exclusive OR* (XOR) adalah metode enkripsi simetris sederhana yang beroperasi pada level bit. Logika XOR menyatakan bahwa jika dua bit yang dibandingkan bernilai sama, hasilnya adalah 0, dan jika berbeda, hasilnya adalah 1 (Adha et al., 2024). Keunggulan utama XOR dalam implementasi sistem *real-time* atau berbasis web adalah kecepatan komputasinya yang tinggi dan sifatnya yang *involuntary*, di mana proses enkripsi dan dekripsi dapat dilakukan menggunakan algoritma dan kunci yang sama. Dengan menerapkan XOR, pesan yang disisipkan ke dalam LSB bukan lagi *plaintext*, melainkan *ciphertext* yang tidak bermakna tanpa kunci dekripsi (Ahmed & Ahmed, 2020).

Pengukuran Kualitas Citra (MSE dan PSNR)

Kualitas citra hasil steganografi (stego-image) perlu diukur untuk memastikan ketidaktampakan (*imperceptibility*) pesan (Utomo Wahyu Mulyono et al., 2023). Dua parameter standar yang digunakan adalah *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR).

1. MSE menghitung rata-rata kuadrat kesalahan kumulatif antara citra asli dan citra stego. Nilai MSE yang rendah menunjukkan kemiripan yang tinggi (Hamrul & Heri, 2022).
2. PSNR digunakan untuk membandingkan tingkat sinyal maksimum terhadap *noise* yang mempengaruhi fidelitas citra. Satuan PSNR adalah desibel (dB). Secara empiris, nilai PSNR di atas 30 dB dianggap dapat diterima, sedangkan nilai di atas 40 dB menunjukkan bahwa distorsi visual sangat sulit dilihat oleh mata telanjang, yang berarti kualitas steganografi sangat baik (Hasanuddin, 2021).

METODE PENELITIAN

Jenis Penelitian

Dalam penelitian ini, diterapkan metode rekayasa perangkat lunak dengan pendekatan kuantitatif deskriptif. Tujuan dari penelitian ini adalah untuk merancang, membangun, serta menguji sebuah aplikasi steganografi gambar digital yang berbasis web, yang mengimplementasikan metode Least Significant Bit (LSB) dipadu dengan algoritma enkripsi Exclusive OR (XOR) untuk menyembunyikan file rahasia di dalam gambar digital.

Pendekatan kuantitatif dipakai untuk menilai kualitas gambar hasil steganografi melalui parameter Mean Squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR), sedangkan pendekatan deskriptif dipergunakan untuk menjelaskan proses sistem, cara kerja aplikasi, serta hasil pengujian yang diperoleh.

JIKUM
JURNAL ILMU KOMPUTER

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

Metode Pengembangan Sistem

Metode yang digunakan dalam pengembangan sistem ini adalah model Waterfall, yang memiliki lima langkah utama, yaitu:

1. Analisis Kebutuhan
2. Perancangan Sistem
3. Implementasi
4. Pengujian
5. Pemeliharaan

Model Waterfall dipilih karena menawarkan tahapan yang terstruktur, sistematis, dan cocok untuk membangun aplikasi dengan kebutuhan yang sudah jelas sejak awal.

Analisis Kebutuhan

Pada tahap ini, dilakukan pengumpulan dan pemeriksaan kebutuhan pengguna untuk sistem steganografi gambar. Kebutuhan utama dari sistem meliputi:

1. Input gambar digital sebagai cover image
2. Input file rahasia yang akan disembunyikan
3. Input password untuk enkripsi XOR
4. Proses enkripsi file memakai algoritma XOR
5. Proses penyisipan data yang telah terenkripsi ke dalam gambar menggunakan metode LSB
6. Proses pengambilan file rahasia dari gambar stego
7. Output dalam bentuk gambar stego dan file hasil pengambilan
8. Informasi mengenai keberhasilan atau kegagalan dalam proses penyisipan dan pengambilan

Perancangan Sistem

Perancangan sistem dilakukan dengan membuat alur kerja aplikasi steganografi berbasis web. Sistem dirancang agar mudah digunakan oleh pengguna dengan antarmuka yang sederhana dan fungsional.

Alur sistem mencakup:

1. Pengguna memilih gambar digital sebagai media penyimpanan.
2. Pengguna memilih file rahasia dan memasukkan password.
3. Sistem melaksanakan enkripsi file menggunakan XOR.
4. Data terenkripsi disisipkan ke dalam gambar dengan metode LSB.
5. Sistem memproduksi gambar stego.
6. Proses pengambilan dilakukan dengan memasukkan gambar stego dan password yang sama.

Implementasi

Penerapan aplikasi dilakukan dengan mengandalkan bahasa pemrograman Python melalui pendekatan aplikasi berbasis web. Proses steganografi terdiri dari dua tahap utama, yaitu penyisipan (embedding) dan pengambilan (extracting).

Tahap embedding dilakukan dengan mengubah bit paling tidak signifikan (LSB) pada nilai piksel gambar. Sebelum disisipkan, file rahasia di-enkripsi menggunakan algoritma XOR untuk meningkatkan tingkat keamanan data Proses extracting dilakukan dengan membaca kembali bit LSB dan mendekripsi XOR menggunakan password yang benar.

Pengujian

Pengujian sistem dilakukan dengan menggunakan metode black-box testing, fokus pada pengujian fungsi utama tanpa mempertimbangkan struktur kode internal.

Pengujian ini mencakup:

1. Pengujian proses penyisipan file
2. Pengujian proses pengambilan file
3. Pengujian kecocokan password
4. Pengujian kualitas gambar hasil steganografi

Pemeliharaan

Proses pemeliharaan dilakukan setelah sistem telah diuji dan dipastikan berfungsi dengan baik. Pemeliharaan meliputi perbaikan kesalahan, peningkatan kinerja sistem, serta pengembangan lebih lanjut seperti penambahan metode steganografi atau algoritma kriptografi lainnya.

JIKUM
JURNAL ILMU KOMPUTER

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

Alat dan Bahan

Alat

1. Bahasa Pemrograman: Python
2. Kerangka Kerja Web: Flask
3. Editor kode: Visual Studio Code
4. Sistem Operasi: Windows
5. Peramban Web

Bahan

1. Gambar digital (PNG dan JPEG)
2. File digital yang berfungsi sebagai pesan tersembunyi
3. Kata Sandi yang digunakan sebagai kunci enkripsi XOR

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui:

1. Tinjauan pustaka dari jurnal nasional dan internasional yang berkaitan dengan steganografi LSB dan XOR
2. Pengamatan terhadap aplikasi steganografi yang sejenis
3. Percobaan penyisipan dan pengumpulan data pada gambar digital

Teknik Analisis Data

1. Data dianalisis dengan metode deskriptif kuantitatif, yaitu:
2. Menghitung nilai MSE dan PSNR
3. Membandingkan kualitas gambar sebelum dan setelah penyisipan
4. Menganalisis tingkat keberhasilan pengambilan file

HASIL DAN PEMBAHASAN

Perancangan dan Pembuatan Aplikasi Steganografi

Proses perancangan dan pengembangan aplikasi steganografi untuk citra digital dalam penelitian ini bertujuan untuk menciptakan sistem yang dapat menyembunyikan file rahasia dengan aman dan tanpa dapat terdeteksi secara visual. Aplikasi ini dirancang berbasis web dengan menggabungkan metode Least Significant Bit (LSB) untuk penyisipan data serta algoritma Exclusive OR (XOR) sebagai metode enkripsi data sebelum proses penyisipan dilakukan.

Tahapan dalam merancang aplikasi steganografi dilaksanakan secara berurutan sebagai berikut:

1. Aplikasi menerima input berupa citra digital yang berfungsi sebagai media penyimpanan (cover image) serta file rahasia yang akan disembunyikan.
2. Pengguna menginputkan password yang akan digunakan sebagai kunci untuk enkripsi dalam algoritma XOR.
3. Sistem melakukan enkripsi pada file rahasia melalui operasi XOR berdasarkan password yang telah dimasukkan.
4. Data yang telah terenkripsi kemudian diubah menjadi bentuk biner dan disisipkan ke dalam bit paling tidak signifikan (LSB) dari masing-masing piksel citra digital.
5. Setelah penyisipan selesai, sistem menghasilkan citra stego yang terlihat hampir sama dengan citra aslinya.
6. Aplikasi juga menyediakan fitur untuk mengekstrak file, di mana pengguna harus memasukkan citra stego dan password yang sama untuk mengambil kembali file rahasia tersebut.
7. Apabila password yang dimasukkan tidak sesuai, maka hasil ekstraksi tidak dapat dikembalikan ke bentuk file yang benar.

Tahapan ini menunjukkan bahwa sistem menerapkan konsep keamanan berlapis, dimana pesan tidak hanya disembunyikan, tetapi juga dilindungi isinya melalui proses enkripsi sebelum dilakukan penyisipan.

Implementasi Sistem

Penerapan aplikasi steganografi dilakukan dengan memperhatikan kebutuhan perangkat keras dan perangkat lunak agar sistem dapat berfungsi dengan baik dan mudah digunakan oleh para pengguna.

Spesifikasi Perangkat Keras (Hardware)

Perangkat keras yang diperlukan untuk menjalankan dan menguji aplikasi steganografi ini disarankan memiliki spesifikasi minimum sebagai berikut:

1. Prosesor: Intel atau AMD Processor
2. Memory (RAM): Minimal 2 GB
3. Media Penyimpanan: Minimal 250 GB ruang kosong
4. Monitor: Resolusi minimal 1024 × 768 piksel

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

5. Perangkat Input: Keyboard dan mouse

Spesifikasi ini dianggap cukup untuk menjalankan aplikasi berbasis web dan melakukan proses enkripsi, penyisipan, serta ekstraksi data tanpa mengalami masalah dalam performa.

Spesifikasi Perangkat Lunak (Software)

Adapun perangkat lunak yang digunakan dalam penerapan sistem mencakup:

1. Sistem Operasi: Windows 7, 8, 10, atau 11
2. Bahasa Pemrograman: Python versi 3. x
3. Framework Web: Flask
4. Browser: Google Chrome atau browser lain yang sejenis
5. Editor Kode: Visual Studio Code

Pemilihan Python dan Flask didasari oleh kemudahan dalam pengembangan, kecepatan pemrosesan, dan fleksibilitas dalam membangun aplikasi web ringan untuk tujuan steganografi.

Alur Kerja Steganografi Metode LSB dan XOR

Proses operasional sistem steganografi pada aplikasi ini terdiri dari dua tahap utama, yakni penyisipan (embedding) dan ekstraksi (extraction).

1. Sistem membaca citra digital yang dipilih oleh pengguna dan mengubahnya menjadi array piksel.
2. File rahasia dienkripsi menggunakan algoritma XOR dengan password yang dimasukkan oleh pengguna.
3. Data hasil enkripsi selanjutnya dikonversi menjadi urutan bit biner.
4. Bit-bit tersebut dimasukkan ke dalam bit LSB setiap piksel citra.
5. Citra yang dihasilkan setelah penyisipan disimpan sebagai stego image.
6. Pada tahap ekstraksi, sistem akan membaca kembali bit LSB dari stego image.
7. Data biner yang diperoleh dekripsi menggunakan algoritma XOR dengan password yang sama untuk mengembalikan file ke bentuk awalnya.

Proses ini menjamin bahwa data rahasia hanya dapat diambil kembali oleh pihak yang mengetahui password yang benar.

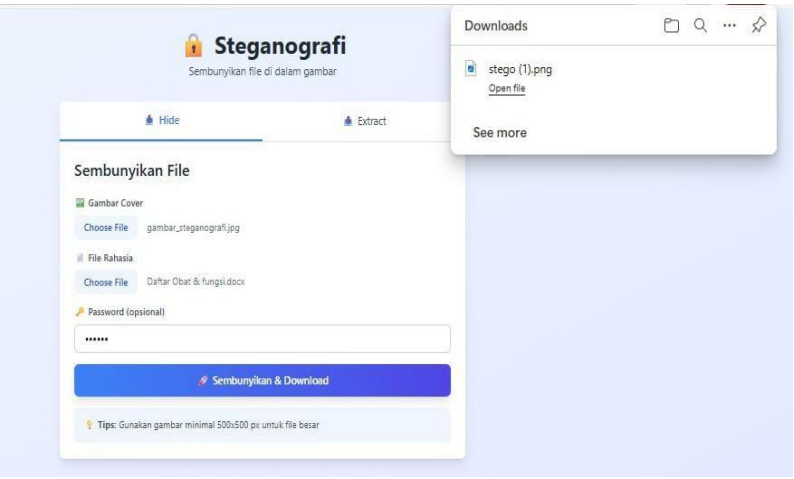

Fig. 1 Antarmuka Penyisipan File (Hide File)

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

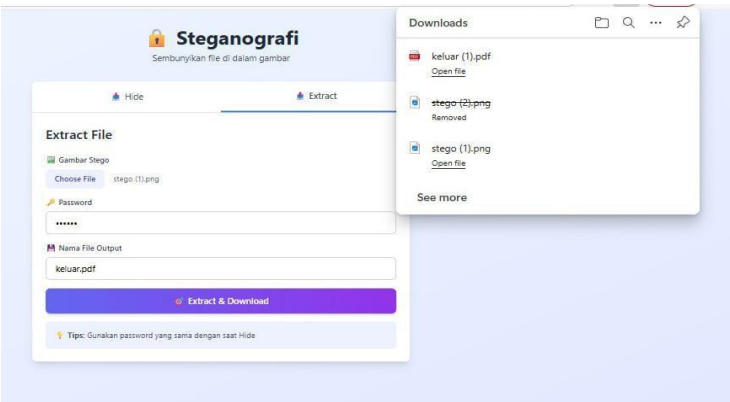

Fig. 2 Antarmuka Ekstraksi File (Extract File)

Hasil pengujian menunjukkan bahwa file rahasia dapat diambil kembali dengan utuh tanpa adanya kerusakan data, asalkan kata sandi yang digunakan dalam proses ekstraksi sama dengan yang digunakan saat penyisipan.

Hasil Pengujian Kualitas Citra

Untuk mengevaluasi kualitas citra yang dihasilkan dari steganografi, digunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Pengujian dilakukan dengan membandingkan citra asli dan citra stego yang dihasilkan setelah proses penyisipan data.

Nilai MSE yang didapat relatif kecil, yang menunjukkan bahwa perbedaan antara citra asli dan citra stego sangat sedikit. Di sisi lain, nilai PSNR yang diperoleh melebihi 40 dB, yang menunjukkan bahwa kualitas visual citra stego sangat baik dan sulit untuk dibedakan oleh penglihatan manusia.

Tabel Hasil Pengujian PSNR dan MSE

Table 1. Hasil Pengujian Kualitas Citra Steganografi

Format	Ukuran File	MSE	PSNR (dB)	Format	Ukuran File
PNG	200 KB	0.42	45.31	PNG	200 KB
PNG	350 KB	0.57	44.12	PNG	350 KB
JPEG	200 KB	0.61	43.87	JPEG	200 KB
JPEG	400 KB	0.74	42.95	JPEG	400 KB

KESIMPULAN

Dari hasil desain, implementasi, dan pengujian aplikasi steganografi untuk citra digital yang sudah dilakukan, bisa ditarik kesimpulan bahwa penggabungan metode Least Significant Bit (LSB) dengan algoritma Exclusive OR (XOR) telah berhasil diimplementasikan dengan baik untuk menyembunyikan dan mengamankan informasi rahasia. Aplikasi yang dibuat mampu menyisipkan file rahasia ke dalam citra digital tanpa menghasilkan perbedaan visual yang berarti antara citra asli dan citra steganografi.

Analisis hasil pengujian menunjukkan bahwa sistem ini dapat melakukan penyisipan dan ekstraksi file dengan baik, asalkan password yang dipakai dalam kedua proses tersebut identik. Penggunaan algoritma XOR sebagai metode enkripsi memberikan tambahan tingkat keamanan, sehingga informasi rahasia yang disisipkan tidak dapat diakses atau digunakan jika password yang dimasukkan tidak benar. Ini membuktikan bahwa menerapkan enkripsi sebelum steganografi bisa meningkatkan keamanan data secara keseluruhan.

Dari segi kualitas citra, nilai Mean Square Error (MSE) relatif kecil, sementara nilai Peak Signal to Noise Ratio (PSNR) melebihi 40 dB. Ini menunjukkan bahwa citra stego memiliki kualitas visual yang sangat baik dan sulit untuk dibedakan dibandingkan citra aslinya oleh mata manusia. Selain itu, hasil uji coba juga menunjukkan bahwa format citra PNG memberikan hasil stego yang lebih memuaskan dibandingkan dengan format JPEG, karena tidak terpengaruh oleh kompresi lossy yang dapat memengaruhi bit LSB.

Secara umum, aplikasi steganografi yang dikembangkan telah mencapai tujuan penelitian, yaitu menciptakan sistem penyembunyian data yang aman, efektif, dan mudah digunakan. Namun, metode LSB masih memiliki beberapa keterbatasan terhadap manipulasi citra seperti pengeditan ulang atau kompresi tambahan. Oleh karena itu, penelitian berikutnya dapat berfokus pada pengembangan metode steganografi yang lebih kuat, dengan mengintegrasikan algoritma enkripsi yang lebih handal, dan memperluas media penyisipan tidak hanya untuk citra digital, tetapi juga untuk audio atau video.

JIKUM
JURNAL ILMU KOMPUTER

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

REFERENSI

Adha, M., Yanto, F., Handayani, L., & Pizaini, P. (2024). Steganografi Gambar Menggunakan Metode Least Significant Bit Pada Citra Dengan Operasi XOR. *Building of Informatics, Technology and Science (BITS)*, *6*(1). https://doi.org/10.47065/bits.v6i1.5262

Ahmed, A., & Ahmed, A. (2020). A Secure Image Steganography using LSB and Double XOR Operations. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 20, Issue 5).

Hamrul, H., & Heri, A. (2022). STEGANOGRAFI BERBASIS CITRA DIGITAL UNTUK MENYEMBUNYIKAN DATA MENGGUNAKAN KOMBINASI MULTI BIT LSB DENGAN HILL CIPHER. In *Jurnal Ilmiah Information Technology d'Computare* (Vol. 12).

Hasanuddin, T. (2021). Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography. *Indonesian Journal of Data and Science (IJODAS)*, *2*(2), 91–102.

Maria Baria Set, F. C., Maria Bana, C. N., Angliadi Anunut, M., Da Costa, D., & Niis, Y. (2022). Penerapan Steganografi LSB dan Enkripsi AES untuk Keamanan Data Rahasia pada Gambar Digital. *Blantika: Multidisciplinary Jornal*, *3*, 2025. https://blantika.publikasiku.id/

Na, M., & Al Jum, im. (2025). *Analisis Pengaruh Kompresi File Pada Media Sosial Terhadap Ketahanan Image Steganografi Pada Metode Least Significant Bit (LSB)* (Vol. 8, Issue 1).

Nandar Pabokory, F., Fitri Astuti, I., & Harsa Kridalaksana, A. (2015). IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD. In *Jurnal Informatika Mulawarman* (Vol. 10, Issue 1).

Nirmala, E., Surya, J., No, K., & Selatan, T. (2023). *Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android*. http://openjournal.unpam.ac.id/index.php/informatika36

Parhusip, S. L., & Sari, R. E. (2024). *Pesan yang Dirahasiakan Menggunakan Algoritma Feal dan Caesar Chiper Disisipkan ke Dalam Gambar Menggunakan Metode Least Significan Bit (LSB)*. http://kti.potensi-utama.ac.id/index.php/JID

Rohmanu, A. (2017). IMPLEMENTASI KRIPTOGRAFI DAN STEGANOGRAFI DENGAN METODE ALGORITMA DES DAN METODE END OF FILE. *Jurnal Informatika SIMANTIK*, *2*(1). www.jurnal.stmikcikarang.ac.id

Ryan Kuncoro, T., & Aditama, R. (2019). *STATMAT (Jurnal Statistik dan Matematika ANALISIS KOMBINASI ALGORITMA KRIPTOGRAFI RSA DAN ALGORITMA STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB) DALAM PENGAMANAN PESAN DIGITAL*. *1*(2).

Utomo Wahyu Mulyono, I., Kusumawati, Y., & Kurnia Ningrum, N. (2023). *Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher* (Vol. 14, Issue 1).