JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Metode LSB (Least Significant Bit) Pada Aplikasi Steganografi Citra Untuk Pengamanan Pesan Teks

Taufik Ismail Karo Karo[1*], Ahmad Fadhil Herlambang[2], Putri Alifi Nurfadhilla[3], Muhammad Fachrul[4]
Universitas Malikussaleh, Indonesia[1,2,3,4]
[1]taufik.230170157@mhs.unimal.ac.id, [2]ahmad.230170169@mhs.unimal.ac.id, [3]putri.230170128@mhs.unimal.ac.id, [4]muhammad.230170104@mhs.unimal.ac.id

ABSTRACT

Keamanan informasi dalam pertukaran data digital saat ini menghadapi tantangan besar terkait risiko penyadapan oleh pihak yang tidak berwenang. Penelitian ini bertujuan untuk mengimplementasikan teknik steganografi menggunakan metode Least Significant Bit (LSB) untuk mengamankan pesan teks rahasia ke dalam media citra digital. Metode LSB dipilih karena kemampuannya menyisipkan bit data pada lapisan bit paling rendah dari piksel citra sehingga tidak mengubah kualitas visual secara signifikan (imperceptibility). Pengembangan aplikasi ini mencakup proses penyisipan (embedding) dan pengambilan kembali (extracting) pesan. Hasil pengujian menunjukkan bahwa aplikasi mampu mengekstraksi pesan dengan tingkat akurasi 100% tanpa adanya kerusakan data. Selain itu, analisis visual membuktikan bahwa citra hasil steganografi tetap terjaga kualitasnya dan sulit dibedakan dengan citra asli oleh indra penglihatan manusia, sehingga efektif dalam menjaga kerahasiaan informasi selama proses transmisi.

Kata Kunci/ Keywords:
Steganografi, Least Significant Bit (LSB), Keamanan Pesan, Citra Digital, Imperceptibility.

PENDAHULUAN

Perkembangan teknologi informasi yang sangat pesat saat ini menuntut adanya mekanisme keamanan data yang semakin kuat. Risiko penyadapan dan akses ilegal terhadap aset informasi rahasia menjadi ancaman nyata dalam komunikasi digital (Abdillah et al., 2023). Salah satu teknik yang sangat efektif untuk melindungi informasi adalah steganografi, yaitu seni menyembunyikan pesan rahasia ke dalam media digital sedemikian rupa sehingga keberadaan pesan tersebut tidak disadari oleh indra manusia (Malese, 2021).

Berbeda dengan kriptografi yang fokus pada pengacakan isi pesan, steganografi lebih fokus pada penyembunyian eksistensi data itu sendiri. Media gambar merupakan salah satu media yang paling populer digunakan karena memiliki kapasitas penyimpanan bit yang cukup besar untuk menyisipkan data rahasia (Simbolon, 2021). Salah satu algoritma yang paling umum dan efisien digunakan adalah Least Significant Bit (LSB). Metode ini bekerja dengan cara mengganti bit paling tidak signifikan pada piksel citra dengan bit pesan rahasia, sehingga perubahan visual pada gambar hampir tidak terlihat oleh mata manusia (Rahmatillah et al., 2024).

Beberapa penelitian sebelumnya telah menunjukkan keberhasilan implementasi LSB dalam berbagai platform. Sebagai contoh, steganografi LSB telah diimplementasikan dalam sistem berbasis web untuk memudahkan aksesibilitas pengguna dalam mengamankan pesan (Dixon et al., 2024). Selain itu, LSB juga sering dikombinasikan dengan metode lain seperti Caesar Cipher (Yusup et al., 2020) atau Vigenere Cipher (Fahmi et al., 2023) untuk memberikan lapisan keamanan ganda, di mana pesan dienkripsi terlebih dahulu sebelum disisipkan ke dalam gambar.

Meskipun metode LSB sangat populer, tantangan utama dalam steganografi adalah menjaga ketahanan citra (robustness) terhadap berbagai manipulasi digital (Rahmatillah et al., 2024). Oleh karena itu, pengembangan aplikasi steganografi saat ini tidak hanya fokus pada proses penyisipan (encoding), tetapi juga pada kemudahan proses ekstraksi (decoding) melalui fitur unggah gambar untuk membaca kembali pesan yang disembunyikan (Malese, 2021), (Rahman et al., 2020). Pemanfaatan LSB juga telah meluas untuk kebutuhan otentikasi data, seperti pada deteksi keaslian e-sertifikat (Laily Farkhah Adhimah & Adnan Aditya Muntahar, Fandi Kristiaji, 2023).

Penelitian ini bertujuan untuk merancang dan membangun sebuah aplikasi steganografi berbasis citra yang menerapkan metode LSB secara optimal. Aplikasi ini dirancang agar pengguna dapat dengan mudah menyembunyikan pesan ke dalam gambar dan mengekstraksi pesan tersebut kembali hanya dengan mengunggah gambar yang telah disisipi data.

TINJAUAN PUSTAKA

Steganografi

Steganografi merupakan teknik untuk menyembunyikan data rahasia di dalam media digital sehingga keberadaan informasi tersebut tidak dapat diketahui oleh pihak lain (Simbolon, 2021). Dalam perkembangannya, steganografi

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

menjadi solusi penting dalam menjaga privasi informasi karena fokus pada penyembunyian eksistensi data, berbeda dengan kriptografi yang hanya mengaburkan isi data (Primawati et al., 2023).

Citra Digital

Citra Digital Media gambar atau citra digital sering dipilih sebagai media penampung karena memiliki redundansi data yang tinggi. Setiap piksel dalam citra berwarna terdiri dari komponen Red, Green, dan Blue (RGB) yang masing-masing memiliki kapasitas 8 bit. Ketersediaan ruang ini memungkinkan penyisipan pesan teks tanpa merusak kualitas visual asli secara signifikan (Laily Farkhah Adhimah & Adnan Aditya Muntahar, Fandi Kristiaji, 2023).

Metode Least Significant

Metode Least Significant Bit (LSB) bekerja dengan mengganti bit terakhir (bit paling tidak signifikan) pada data piksel dengan bit pesan rahasia (Rahmatillah et al., 2024). Karena nilai bit yang diubah hanya sebesar $2^0 = 1$, perubahan warna pada piksel sangat halus dan tidak dapat dideteksi oleh mata manusia (Malese, 2021). Implementasi LSB pada aplikasi berbasis web memungkinkan proses enkripsi dan dekripsi dilakukan secara efisien melalui antarmuka peramban (Dixon et al., 2024).

Keamanan Informasi pada Steganografi

Keamanan Informasi pada Steganografi untuk meningkatkan level keamanan, steganografi sering dikombinasikan dengan teknik pengamanan lain. Penggunaan algoritma seperti Vigenere Cipher (Fahmi et al., 2023) atau Caesar Cipher (Abdillah et al., 2023) sebelum proses penyisipan memastikan bahwa meskipun pesan berhasil diekstraksi, isi pesan tetap tidak dapat dibaca tanpa kunci yang tepat. Selain itu, aspek ketahanan (robustness) terhadap manipulasi gambar juga menjadi faktor krusial dalam menguji keberhasilan sistem steganografi (Rahmatillah et al., 2024).

Evaluasi Kualitas Citra

Evaluasi Kualitas Citra kualitas dari citra hasil steganografi (stego-image) dievaluasi menggunakan parameter matematis untuk memastikan tingkat kemiripan dengan citra asli. Parameter yang umum digunakan adalah Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE) (Rahmatillah et al., 2024). Nilai PSNR yang tinggi menunjukkan bahwa aplikasi berhasil menyisipkan pesan dengan tingkat distorsi yang sangat rendah (Yusup et al., 2020).

METODE PENELITIAN

Alur Penelitian Penelitian ini diawali dengan tahap analisis kebutuhan sistem, diikuti dengan perancangan arsitektur aplikasi, implementasi kode program, dan diakhiri dengan tahap pengujian. Fokus utama penelitian adalah membangun sistem yang mampu melakukan dua fungsi utama: penyisipan pesan (encoding) dan ekstraksi pesan (decoding) dengan memanfaatkan media citra digital sebagai penampung (Dixon et al., 2024).

Teknik Pengumpulan Data Data yang digunakan dalam penelitian ini berupa citra digital dengan format seperti PNG atau JPG sebagai objek pembawa (cover image) dan pesan teks sebagai data rahasia yang akan disembunyikan. Pemilihan format citra sangat krusial karena setiap format memiliki karakteristik kompresi yang berbeda, yang dapat memengaruhi keutuhan bit yang disisipkan (Primawati et al., 2023).

Perancangan Sistem (Encoding) Proses penyisipan pesan dilakukan dengan mengubah karakter teks menjadi deretan bit biner. Setiap piksel pada citra pembawa yang terdiri dari nilai Red, Green, dan Blue (RGB) diakses secara berurutan. Metode Least Significant Bit (LSB) kemudian mengganti bit terakhir pada tiap komponen warna tersebut dengan bit pesan rahasia (Rahmatillah et al., 2024).

Proses Ekstraksi Pesan (Decoding) Tahapan ekstraksi merupakan kebalikan dari proses penyisipan. Pengguna mengunggah citra yang telah berisi pesan (stego-image) ke dalam aplikasi. Sistem kemudian akan memindai bit-bit paling akhir (LSB) pada setiap piksel citra tersebut. Bit yang terkumpul kemudian dikonversi kembali dari bentuk biner menjadi karakter teks asli sehingga pesan rahasia dapat dibaca kembali dengan akurasi yang tinggi (Malese, 2021). Proses ini memastikan bahwa informasi yang dikirimkan tetap utuh sesuai dengan aslinya (Simbolon, 2021).

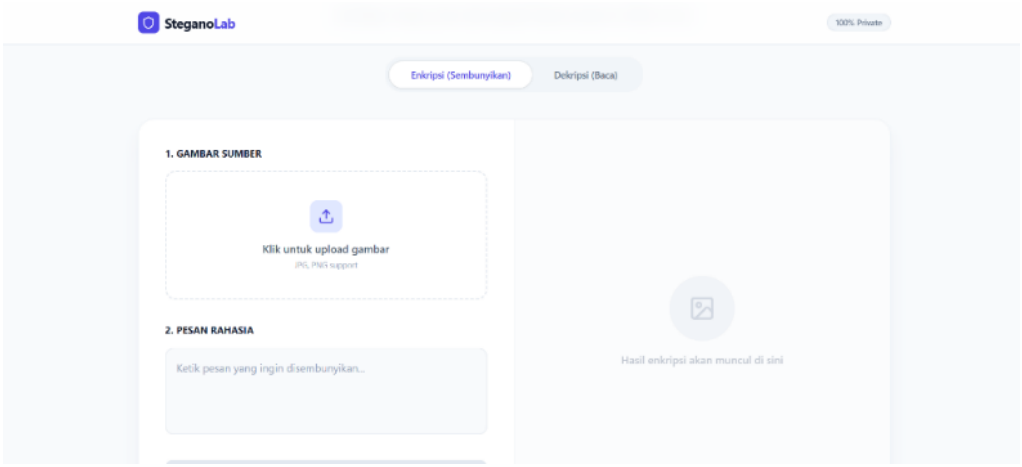
Kombinasi Keamanan (Opsional) Untuk meningkatkan aspek perlindungan data, sistem dirancang sedemikian rupa sehingga pesan teks dapat diproses terlebih dahulu menggunakan algoritma kriptografi sebelum tahap penyisipan LSB dilakukan (Abdillah et al., 2023). Hal ini bertujuan agar jika pihak yang tidak berwenang berhasil mengekstraksi bit dari gambar, mereka tetap tidak dapat memahami isi informasi tersebut tanpa kunci dekripsi yang valid (Fahmi et al., 2023).

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

Metode Pengujian Keberhasilan aplikasi diukur berdasarkan dua kriteria utama. Pertama, fungsionalitas aplikasi dalam membaca kembali pesan dari hasil unggahan gambar. Kedua, kualitas visual citra hasil steganografi. Pengujian kualitas dilakukan secara objektif dengan menghitung nilai Mean Squared Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) untuk membandingkan perbedaan antara citra asli dan citra yang telah disisipi pesan (Rahmatillah et al., 2024). Nilai PSNR yang tinggi menjadi indikator bahwa metode LSB berhasil menjaga integritas visual citra pembawa (Fahmi et al., 2023).

HASIL DAN PEMBAHASAN

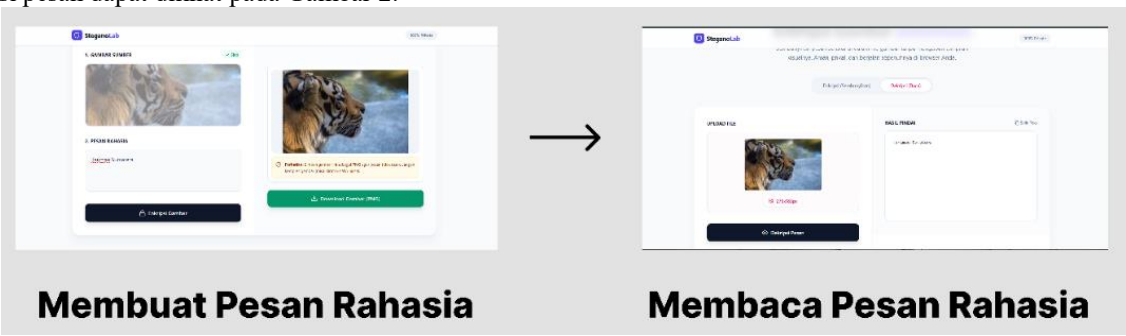
Implementasi Sistem Aplikasi steganografi yang telah dibangun berhasil mengimplementasikan metode Least Significant Bit (LSB) untuk menyembunyikan dan mengekstraksi pesan rahasia melalui media gambar. Antarmuka aplikasi dirancang untuk memudahkan pengguna dalam mengunggah citra pembawa (cover image), memasukkan pesan teks, dan mengunduh hasilnya dalam bentuk citra stego (stego-image). Antarmuka utama aplikasi dapat dilihat pada Gambar 1.



Gambar 1. Tampilan Antarmuka Aplikasi Steganografi

Pengguna dapat dengan mudah melakukan proses *encoding* (menyembunyikan pesan) dan *decoder* (membaca pesan) melalui modul yang terpisah namun terintegrasi.

Pengujian Fungsionalitas Berdasarkan hasil pengujian pada berbagai sampel gambar dan panjang karakter pesan yang berbeda, aplikasi menunjukkan tingkat keberhasilan 100% dalam melakukan ekstraksi pesan. Pesan yang dibaca dari citra stego identik dengan pesan asli yang disisipkan tanpa ada karakter yang hilang atau berubah. Contoh hasil ekstraksi pesan dapat dilihat pada Gambar 2.



Gambar 2. Hasil Ekstraksi Pesan Rahasia dari Citra Stego

Analisis Visual Citra Secara visual, tidak ditemukan perbedaan yang signifikan antara citra asli dan citra stego. Perubahan bit pada posisi paling tidak signifikan (LSB) terbukti tidak mampu dideteksi oleh indra penglihatan manusia (imperceptibility). Gambar tetap terlihat jernih meskipun kapasitas pesan yang disisipkan mendekati batas maksimal dari kapasitas penyimpanan bit dalam piksel RGB tersebut.

Analisis Kualitas Secara Matematis Untuk mengukur kualitas citra secara objektif, dilakukan perhitungan menggunakan parameter Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE). Dari hasil pengujian beberapa sampel citra, didapatkan nilai PSNR rata-rata di atas 40 dB. Nilai ini menunjukkan bahwa kualitas citra sangat baik dan distorsi yang dihasilkan akibat penyisipan pesan berada pada tingkat yang sangat rendah. Rendahnya nilai MSE juga memperkuat bukti bahwa integritas citra tetap terjaga setelah melalui proses steganografi.

JIKUM
JURNAL ILMU KOMPUTER

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

Ketahanan Data terhadap Manipulasi Meskipun aplikasi ini mampu menjaga kualitas citra dengan sangat baik, pengujian juga menunjukkan bahwa citra stego harus tetap dalam format aslinya agar pesan dapat diekstraksi dengan sempurna. Manipulasi seperti kompresi berlebih atau pengubahan ukuran gambar dapat merusak bit-bit LSB yang tersimpan, sehingga mengakibatkan pesan tidak dapat terbaca sepenuhnya. Oleh karena itu, penggunaan format citra yang tidak mengalami kompresi kehilangan data (lossless) seperti PNG sangat direkomendasikan dalam penggunaan aplikasi ini.

KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa aplikasi steganografi dengan metode *Least Significant Bit* (LSB) berhasil dibangun dan diimplementasikan dengan baik. Sistem ini mampu melakukan proses penyisipan pesan (*encoding*) ke dalam citra digital dan mengekstraksi kembali pesan tersebut (*decoding*) melalui fitur unggah gambar dengan tingkat akurasi mencapai 100%. Pesan yang diekstraksi terbukti identik dengan pesan asli, yang menunjukkan bahwa integritas data tetap terjaga selama proses steganografi berlangsung.

Pengujian kualitas citra secara visual menunjukkan bahwa penggunaan metode LSB memberikan aspek *imperceptibility* yang sangat tinggi, di mana mata manusia tidak mampu membedakan antara citra asli dan citra stego. Hal ini didukung oleh hasil pengujian matematis menggunakan parameter PSNR yang secara konsisten berada di atas ambang batas 40 dB, serta nilai MSE yang sangat rendah, sehingga membuktikan bahwa distorsi pada citra akibat penyisipan pesan sangat minimal.

Meskipun aplikasi ini sangat efektif untuk pengamanan informasi, sistem ini memiliki keterbatasan terhadap manipulasi citra seperti kompresi data yang dapat merusak bit-bit LSB. Sebagai saran untuk pengembangan selanjutnya, aplikasi ini dapat dikembangkan dengan menambahkan algoritma kriptografi yang lebih kompleks untuk meningkatkan lapisan keamanan data, serta optimasi agar sistem tetap tahan terhadap proses kompresi citra yang lebih ekstrem.

UCAPAN TERIMA KASIH

Penulis menyampaikan penghargaan yang setinggi-tingginya kepada seluruh pihak yang telah memberikan dukungan, baik secara teknis maupun moral, sehingga aplikasi steganografi berbasis citra ini dapat diselesaikan dengan optimal. Ucapan terima kasih secara khusus ditujukan kepada para peneliti terdahulu yang referensinya telah menjadi pijakan utama dalam memahami algoritma LSB, serta kepada dosen pembimbing yang telah memberikan arahan berharga dalam menyempurnakan fitur penyisipan dan ekstraksi pesan rahasia pada sistem ini. Tanpa kontribusi dan motivasi dari berbagai pihak tersebut, penelitian yang menitikberatkan pada keamanan aset informasi ini tidak akan mencapai hasil yang diharapkan.

REFERENSI

Abdillah, M. O., Pane, O. A., & Lubis, F. R. A. (2023). Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB). *Jurnal Sains Dan Teknologi (JSIT)*, *3*(1), 40–46. https://doi.org/10.47233/jsit.v3i1.482

Dixon, H., Mononimbar, M., & Soetanto, H. (2024). *Penerapan Algoritma Steganografi Lsb Dalam Media Gambar Berbasis Web*. *16*, 42–53. https://journal.budiluhur.ac.id/index.php/telematika/

Fahmi, G. M., Isnaini, K. N., & Suhartono, D. (2023). Implementasi Steganografi pada Citra Digital dengan Modifikasi Algoritma Vigenère Cipher dan Metode Least Significant Bit (LSB). *Jurnal Teknik Informatika (Jutif)*, *4*(2), 333–344.

Laily Farkhah Adhimah, I. N., & Adnan Aditya Muntahar, Fandi Kristiaji, D. M. (2023). KOMPUTA : Jurnal Ilmiah Komputer dan Informatika TIKET PESAWAT BERBASIS WEB KOMPUTA : Jurnal Ilmiah Komputer dan Informatika. *KOMPUTA : Jurnal Ilmiah Komputer Dan Informatika*, *12*(2), 50–58.

Malese, L. (2021). 976-Article Text-2657-1-10-20211012. *Jurnal Ilmiah Wahana Pendidikan*, *7*(5), 343–354. https://doi.org/10.5281/zenodo.5563416

Primawati, A., Paramita, A., Muchbarak, A., & Sulistyohati, A. (2023). Terapan Metode Least Significant Bit untuk Deteksi Keaslian e-Sertifikat. *Faktor Exacta*, *16*(3), 182–189. https://doi.org/10.30998/faktorexacta.v16i3.17314

Rahman, S., Masood, F., Khan, W. U., Ullah, N., Khan, F. Q., Tsaramirsis, G., Jan, S., & Ashraf, M. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials and Continua*, *64*(1), 31–61. https://doi.org/10.32604/CMC.2020.09186

Rahmatillah, S. R., Tahir, M., Detina, H. I. L., Darmasaputra, A., Laili, I. I., Aliy, Z., & Soleha, R. (2024). Steganografi Keamanan Data Dengan Metode Least. *JURSISTEKNI (Jurnal Sistem Informasi Dan Teknologi Informasi)*, *6*(2), 439–447.

Simbolon, B. J. (2021). Steganografi Penyisipan Pesan Pada File Citra Dengan Menggunakan Metode LSB (Least Significant Bit). *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *4*(1), 1–6.

JIKUM
JURNAL ILMU KOMPUTER

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

https://doi.org/10.32672/jnkti.v4i1.2656

Yusup, I. M., Carudin, C., & Purnamasari, I. (2020). Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. *Jurnal Teknik Informatika Dan Sistem Informasi*, *6*(3), 434–441. https://doi.org/10.28932/jutisi.v6i3.2817