JIKUM
JURNAL ILMU KOMPUTER

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

Perancangan dan Implementasi Aplikasi Steganografi Gambar Berbasis Web Menggunakan Metode Least Significant Bit (LSB)

Atikah Sari[1], Meutia Rahma Kartika[2*], Cut Mutiara Jannah[3] , Fajar Wahyudi Batubara[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]atikah.230170006@unimal.ac.id, [2]meutia.230170026@unimal.ac.id, [3]cut.230170033@mhs.unimal.ac.id,
[4]fajar.230170172@unimal.ac.id

ABSTRACT

Information security is an important aspect of digital data exchange over the internet. In addition to cryptography, steganography offers an alternative approach by concealing secret messages within digital media so that their existence is difficult to detect. This study aims to implement a web-based digital image steganography system using the Least Significant Bit (LSB) method. The application is developed using HTML, CSS, and JavaScript, enabling users to embed and extract text messages directly through a web browser. The LSB method is applied by modifying the Least significant bits of each pixel byte in the digital image. The experimental results show that secret messages can be successfully embedded an extracted without causing significant visual differences between the original image and the stego-image. Therefore, the LSB methode is proven to be effective for simpel web-based steganography applications, although is still has limitations against certain image manipulations.

Keywords:
Steganography, Digital Image, Least Significant Bit, Information Security, Web-Based Application.

PENDAHULUAN

Perkembangan teknoligi informasi dan komunikasi telah meningkatkan kebutuhan akan sistem keamanan data yang andal. Informassi yang dikirimkan melalui jaringan internet memiliki risiko tinggi terhadap penyadapan, manipulasi, maupun pencurian data. Oleh karena itu, diperlukan metode pengamanan informasi yang tidak hanya melindungi isi pesan, tetapi juga menyamarkan keberadaan pesan tersebut. Kriptografi merupakan metode yang umum digunakan, namun keberadaan pesan terenkripsi sering kali mudah dikenali sehingga berpotensi menimbulkan kecurigaan (Firdaus et al., 2025).

Steganografi menjadi solusi alternatif pengamanan data dengan cara menyembunyikan pesan rahasia ke dalam suatu media pembawa, seperti gambar, audio, atau video, sehingga pesan tersebut tidak terlihat secara langsung oleh pihak yang tidak berwenang. Berbeda dengan kriptografi yang menyamarkan isi pesan, steganografi berfokus pada penyamaran keberadaan sehingga tidak menimbulkan kecurigaan.

Pada penelitian ini, penulis mengembangkan aplikasi steganografi gambar berbasis web menggunakan metode Last Significant Bit (LSB). Di antara berbagai teknik steganografi citra, metode Least Signifikan Bit (LSB) merupakan salah satu metode yang paling sederhana dan banyak digunakan karena memiliki kompleksitas rendah serta tidak menyebabkan perubahan visual yang signifikan (Hasan et al., 2020).

Seiring dengan perkembangan teknologi web, implementasi steganografi tidak lagi terbatas pada aplikasi desktop, melainan dapat dikembangkan berbasis web agar lebih mudah diakses dan digunakan. Oleh karena itu penelitian ini bertujuan untuk mengimplementasikan steganografi citra digital berbasis web menggunakan metode LSB dengan memanfaatkan teknologi HTML, CSS, dan JavaSript. Aplikasi ini dirancang sederhana, mudah digunakan, dan dapat dijalankan langsung melalui browser sehingga cocok digunakan sebagai media pembelajaran maupun tugas akademik.

TINJAUAN PUSTAKA

Steganografi

Steganografi berasal dari bahasa Yunani, yaitu stegos yang berarti tersembunyi dan graphia yang berarti tulisan. Steganografi didefinisikan sebagai teknik penyembunyian pesan rahasia di dalam suatu media penampung sehingga keberadaan pesan tersebut sulit dideteksi (Muhammad et al., n.d.). Fokus utama steganografi adalah imperceptibility, yaitu kemampuan sistem untuk menjaga kualitas media penampung agar tetap terlihat normal (Ngurah et al., 2024). Aspek lain yang penting adalah capacity (daya tampung) dan robustness (ketahanan terhadap manipulasi) (Yanti & Budayawan, 2023).

Steganografi Citra Digital

Steganografi digital memanfaatkan struktur pixel citra yang tersusun atas kanal warna RGB. Setiap kanal warna memiliki bit-bit penyusun yang dapat dimodifikasi tanpa memengaruhi persepsi visual manusia secara signifikan,

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

terutama pada bit-bit dengan bobot rendah (Hasan et al., 2020). Citra digital dalam format tanpa kompresi lossy seperti BMP dan PNG lebih disukai karena dapat menjaga integritas pesan yang disisipkan.

Metode Least Signifikan Bit (LSB)

Metode LSB bekerja dengan mengganti bit paling tidak signifikan (bit terakhir) dan nilai pixel dengan bit pesan rahasia. Pada citra 24-bit RGB, setiap pixel terdiri dari 3 byte (masing-masing untuk Red, Green,Blue). Dengan memanipulasi 1 LSB dari setiap byte, dapat disisipkan 3 bit data per pixel. Penelitian menunjukkan bahwa metode ini efektif dalam menyembunyikan pesan teks dengan distorsi visual yang sangat rendah (Hasan et al., 2020), (Firdaus et al., 2025).

Steganalisis dan Keamanan LSB

Meskipun sederhana, metode LSB standar rentan terhadap serangan steganalysis, seperti analisis statistik (Chi-Square) yang dapat mendeteksi ketidakseimbangan distribusi bit LSB (Maulidina & Idris, 2024). Untuk meningkatkan keamanan, LSB sering dikombinasikan dengan teknik kriptografi seperti Vigenere Chiper (Fahmi et al., 2023), (Yanti & Budayawan, 2023) atau enkripsi AES (Firdaus et al., 2025), serta penggunaan pola penyisipan acak (pseudorandom embedding) untuk menyulitkan deteksi.

Implementasi Berbasis Web

Pengembangan aplikasi berbasis web untuk steganografi menawarkan kemudahan akses dan penggunaan lintas platform. Teknologi HTML, CSS, dan JavaScript memungkinkan manipulasi pixel gambar secara langsung di sisi klien (client-side) tanpa perlu pengolahan di server, sehingga meningkatkan kecepatan dan privasi (Dimas et al., 2024), (Adhimah et al., 2023). Pendekatan ini menjadikan aplikasi ringan dan dapat diakses melalui berbagai perangkat hanya dengan menggunakan web browser.

Penelitian Terdahulu

Penelitian mengenai steganografi citra digital berbasis Least Significant Bit (LSB) masih banyak dilakukan dalam beberapa tahun terakhir. (Hasan et al., 2020) menganalis perubahan histogram pada citra grayscale hasil penyisipan pesan menggunakan metode LSB dan menyimpulkan bahwa perubahan visual yang dihasilkan relatif kecil, sehingga pesan sulit dideteksi secara kasat mata.

Penelitian lain menunjukkan bahwa metode LSB sering dikombinasikan dengan teknik tambahan untuk meningkatkan keamanan. (Firdaus et al., 2025) mengintegrasikan metode LSB dengan enkripsi AES untuk memperkuat perlindungan pesan tersembunyi. Sementara itu, (Fahmi et al., 2023) mengombinasikan LSB dengan algoritma kriptografi klasi klasik untuk meningkatkan kerahasiaan data yang disisipkan.

Berdasarkan penelitian-penelitian tersebut, metode LSB masih relevan digunakan, khususnya aplikasi steganografi sederhana. Namun, sebagian besar penelitian terdahulu belum mengimplementasikan metode ini dalam aplikasi berbasis web secara langsung, sehingga penelitian ini difokuskan pada pengembangan steganografi LSB berbasis web yang mudah diakses pengguna.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini menggunakan metode eksperimental dengan pendekatan rekayasa perangkat lunak, yaitu perancangan dan implementasi aplikasi steganografi citra berbasis web.

Perangkat dan Teknologi

Aplikasi pengembangan menggunakan HTML sebagai struktur antarmuka, CSS untuk desain tampilan, serta JavaScript untuk mengimplementasikan algoritma steganografi LSB. Media penumpang berupa citra digital berformat PNG dipilih karena tidak menggunakan kompresi Lossy.

Prosedur Encoding

Pesan teks dikonversi menjadi represantasi biner 8-bit per karakter. Bit-bit tersebut kemudian disisipkan ke dalam bit LSB setiap byte piksel citra. Untuk menandai akhir pesan, digunakan karakter khusus sebagai terminator, sehingga proses decoding dapat dihentikan secara otomatis (Fahmi et al., 2023).

Prosedur Decoding

Proses decoding dilakukan dengan membaca bit LSB dari setiap byte piksel dan mengonversinya kembali menjadi karakter ASCII. Proses ini dihentikan ketika terminator pesan terdeteksi (Hasan et al., 2020).

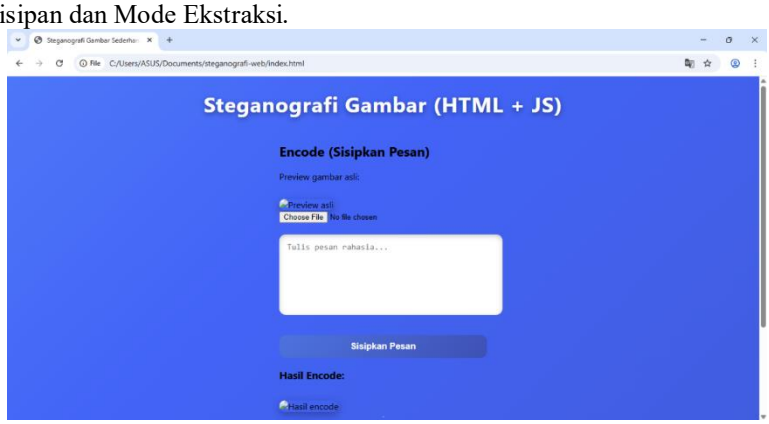
JIKUM
JURNAL ILMU KOMPUTER

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

HASIL DAN PEMBAHASAN

Implementasi Antarmuka Pengguna (UI)

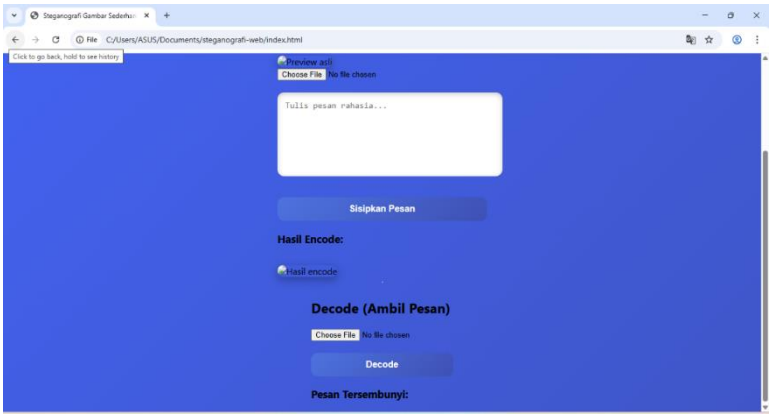
Aplikasi steganografi berbasis web ini telah berhasil diimplementasi dengan antarmuka yang sederhana dan intuitif menggunkan HTML, CSS, dan JavaScript di lingkungan VS Code. Antarmuka utama terbagi menjadi 2 bagian utama yaitu Mode Penyisipan dan Mode Ekstraksi.



Gambar 1. Tampilan Encode

Mode Penyisipan berisi:

1. Input file untuk memilih gambar cover (format PNG/JPG).
2. Texarea untuk memasukkan pesan teks rahasia.
3. Tombol "Sisipkan Pesan" untuk menjalankan proses encoding.
4. Area pratinjau untuk menampilkan cover image dan stego-image hasil proses.
5. Tombol untuk mengunduh stego-image.



Gambar 2. Tampilan Decode

Mode Ekstraksi berisi:

1. Input file untuk memilih stego-image.
2. Tombol "Ekstrak Pesan" untuk menjalankan proses decoding.
3. Area untuk menampilkan pesan teks rahasia yang berhasil diekstraksi.

Antarmuka dibangun responsive menggunkan CSS Grid dan Flexbox, sehingga dapat diakses dengan baik dari perangkat desktop maupun mobile.

Hasil Pengujian Fungsionalitas

Pengujian black box pada semua komponen antarmuka dan fungsi logika JavaScript menunjukkan bahwa aplikasi berjalan sesuai dengan yang diharapkan. Proses encoding dan decoding berhasil dilakukan sepenuhnya di sisi klien (client-side) menggunkan JavaScript, tanpa memerlukan komunikasi dengan server, yang menjamin kecepatan dan kerahasiaan proses.

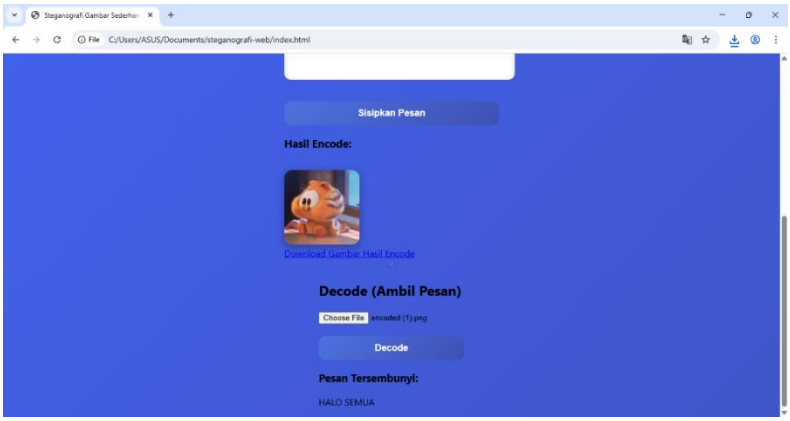
Hasil Penyisipan dan Ekstraksi Pesan

Eksperimen dilakukan dengan menggunakan beberapa gambar cover berukuran berbeda dan pesan teks dengan panjang bervariasi. Berikut adalah contoh tampilan hasil encoding dan decoding dan hasilnya menunjukkan bahwa:

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

Gambar 3. Tampilan Hasil Encode

Pada contoh ini, pesan "HALO SEMUA" berhasil disisipkan ke dalam gambar cover. Hasil stego-image dapat diunduh dan digunakan untuk proses ekstraksi.



Gambar 4. Tampilan Hasil Decode

Proses decoding berhasil mengekstraksi pesan "HALO SEMUA" dari srego-image tanpa kesalahan karakter. Secara keseluruhan, hasil eksperimen menunjukkan bahwa:

1. Pesan teks berhasil disisipkan ke dalam semua gambar cover yang diuji.
2. Proses ekstraksi dari stego-image yang dihasilkan selalu berhasil mengembalikan pesan teks yang identik dengan pesan asli, tanpa kesalahan karakter, selama format gambar tidak diubah atau dikompresi ulang.
3. Kapasitas penyisipan maksimum bergantung pada jumlah pixel gambar. Untuk gambar dengan ukuran 800 X 600 pixel (480,000 pixel), dan menggunakan 3 LSB per pixel (RGB), kapasitas teoritis adalah 480,000 pixel * 3 bit/pixel = 1,440,000 bit = 180,000 byte ~ 176 KB teks. Dalam praktiknya, batas ini lebih dari cukup untuk pesan teks biasa.

Analisis Kualitas Visual (Imperceptibility)

Imperceptibility adalah parameter kunci kesuksesan steganografi. Analisis dilakukan dengan dua cara:

1. Analisis Visual:
   Secara kasat mata, tidak terdapat perbedaan yang nyata antar cover image dan stego-image untuk semua sample yang diuji. Modifikasi pada bit LSB menghasilkan perubahan intensitas warna yang sangat halus, di bawah ambang batas persepsi manusia.
2. Analisis Kuantitatif dengan PSNR:
   Untuk mengukur distorsi secara objektif, dihitung nilai Peak Signal-to-Noise Ratio (PSNR) antara gambar asli dan gambar stego. PSNR dihitung menggunakan rumus:

$$PSNR = 10 * \log10 (MAX\_I^2 / MSE)$$

Dimana MAX_I adalah nilai intensitas maksimum (255 untuk gambar 8-bit), dan MSE (Mean Squared Error) adalah rata-rata kuadrat selisih intensitas semua pixel. Hasil perhitungan PSNR untuk beberapa percobaan berkisar

JIKUM
JURNAL ILMU KOMPUTER

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

antara **45 dB hingga 60 dB.** Nilai PSNR diatas 40 dB secara umum diindikasikan sebagai kualitas yang sangat baik dan tidak terlihat perbedaannya oleh mata manusia. Hasil ini membukktikan bahwa implemntasi LSB pada aplikasi web ini memenuhi kriteria imperceptibility.

Pembahasan Terkait Keamanan dan Keterbatasan

Meskipun berhasil dalam penyembunnyian pesan, aplikasi ini mengimplementasikan LSB standar yang memiliki keterbatasan keamanan:

1. Rentan terhadap Steganalisis Statistik:
   Metode LSB dapat dideteksi melalui uji statistik seperti Chi-square yang menganalisis distribusi bit LSB.
2. Fragility:
   Pesan yang disisipkan sangat rentan hilang atau rusak jika stego-image mengalami proses kompresi lossy (seperti konversi ke JPEG), cropping, resizing, atau penyuntingan gambar lainnya. Oleh karena itu, penggunaan format PNG dan anjuran untuk tidak memanipulasi gambar hasil sangat penting.

Aplikasi ini berhasil mencapai tujuan perancangan dan implementasi steganografi berbasis web yang sederhana dan fungsional. Hasil yang diperoleh menunjukkan bahwa pendekatan berbasis web dengan teknologi front-end standar dapat menjadi alternatif yamg layak untuk implrmrntasi steganografi dasar. Hasil penelitian juga menunjukkan bahwa citra hasil penyisipan pesan tidak memngalami perbedaan visual yang signifikan dibandingkan citra asli. Temuan in sejalan dengan penelitian sebelumnya yang menyatakan bahwa metode LSB mampu mempertahankan kualtitas citra digital dengan nilai PSNR yang baik (Yanti & Budayawan, 2023), (Terapan et al., 2025).

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa aplikasi steganografi gambar berbasis web menggunakan metode Least Significant Bit (LSB) telah berhasil dirancang dan diimplementasikan. Aplikasi ini dikembangkan dengan teknologi HTML, CSS, dan JavaSceipt dalam lingkungan Visual Studio Code, memungkinkan pengguna untuk menyisipkan dan mengekstraksi pesan teks rahasia ke dalam gambar digital secara langsung melalui web browser tanpa memerlukan instalasi perangkat lunak tambahan. Hasil pengujian menunjukkan bahwa aplikasi berfungsi dengan baik dalam proses penyisipan dan ekstraksi pesan, serta menghasilkan kualitas visual stego-image yang terjaga dengan sangat baik, sebagaimana dibuktikan melalui analisis visual dan perhitungan PSNR yang mencapai nilai di atas 45 dB. Dengan demikian, metode LSB terbukti efektif untuk diimplemntasikan dalam aplikasi steganografi berbasis web yang sederhana, cocok digunakan sebagai media pembelajaran konsep dasar steganografi maupun alat bantu pengamanan informasi dengan Tingkat risiko rendah.

REFERENSI

Adhimah, L. F., Nurhafiyah, I., Muntahar, A. A., Kristiaji, F., & Mustofa, D. (2023). *KOMPUTA : Jurnal Ilmiah Komputer dan Informatika IMPLEMENTASI APLIKASI STEGANOGRAFI BERBASIS WEB KOMPUTA : Jurnal Ilmiah Komputer dan Informatika*. *12*(2), 100–108.

Dimas, I. W., Saputra, W., & Santi, I. G. (2024). *Perancangan Sistem Penyisipan Pesan pada Gambar dengan Metode Least Significant Bit (LSB) Berbasis Website*. *2*, 305–310.

Fahmi, G. M., Isnaini, K. N., & Suhartono, D. (2023). *IMPLEMENTATION OF STEGANOGRAPHY ON DIGITAL IMAGE WITH MODIFIED VIGENERE CIPHER ALGORITHM AND LEAST SIGNIFICANT BIT (LSB) METHOD MODIFIKASI ALGORITMA VIGENERE CIPHER DAN METODE LEAST SIGNIFICANT BIT (LSB)*. *4*(2), 333–344.

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

Hasan, N. F., Dengen, C. N., & Ariyus, D. (2020). *Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale*. *x*(x), 20–29.

Maulidina, J. R., & Idris, N. Bin. (2024). *IMPLEMENTASI STEGANOGRAFI DAN STEGANALISIS MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT) PADA FILE GAMBAR*. *1*(1).

Muhammad, A., Agus, A., Mujahid, M. R., Negeri, U., & Makassar, K. (n.d.). *The Security of Recent LSB Steganography Algorithms for Protecting Secret Text Messages*. *1*, 12–16.

Ngurah, I. G., Ananda, F., & Eka, A. (2024). *Penerapan Teknik Steganografi LSB pada Format Gambar Modern*. *2*, 673–680.

Terapan, S., Rekayasa, T., Lunak, P., Vokasi, F., & Del, I. T. (2025). *Implementasi Keamanan Perangkat Lunak Menggunakan Algoritma Kriptografi dan Steganografi berbasis Web*. *3*(1).

Yanti, F., & Budayawan, K. (2023). *Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb)*

JIKUM
JURNAL ILMU KOMPUTER

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

dalam Pengamanan Informasi pada Citra Digital Penggunaan teknologi sebagai sarana dalam penyampaian informasi . P - ISSN : 2302-3295. *11*(1).