JIKUM
JURNAL ILMU KOMPUTER

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

Pengembangan Sistem Steganografi Berbasis Web Menggunakan Metode Least Significant Bit (LSB)

Aiman Fawwaz [1*], Alifmulya Rahman [2], Muhammad Akbar [3], Rahmad Hidayah Damanik [4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1] aiman.230170117@mhs.unimal.ac.id, [2]alifmulya.230170101@mhs.unimal.ac.id,
[3]muhammad.210170235@mhs.unimal.ac.id, [4]rahmad.230170109@mhs.unimal.ac.id

ABSTRACT

Concealing digital information within images has become increasingly important with the growing demand for data security in the digital era. This research develops a web-based steganography system using the Least Significant Bit (LSB) method to hide secret messages within digital images. The system is designed with a user-friendly web interface featuring two main functions: (1) "Hide Message" feature to embed secret messages into images and (2) "Extract Message" feature to extract hidden messages from stego-images. The implementation includes optional security features with password protection, enabling users to perform encoding and decoding processes without requiring specialized technical expertise. Modern web technologies are utilized to ensure accessibility, fast processing speed, and preservation of image quality after message embedding. System testing includes functionality evaluation, image quality analysis using Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) metrics, and user experience testing. Research results demonstrate that the system successfully extracts messages with perfect accuracy ("yok kerja yok") while maintaining image visual quality. The system can be applied in secret communication applications, digital watermarking, and intellectual property protection. In conclusion, the development of this web-based steganography system provides a practical and accessible solution to protect digital information privacy through a user-friendly interface suitable for all user levels.

Keywords: *steganography, LSB, web application, image quality, PSNR, digital data security, message extraction, web interface*

PENDAHULUAN

Perkembangan teknologi internet dan komputasi cloud mendorong semakin banyaknya informasi sensitif yang disimpan dan ditransmisikan melalui jaringan digital. Ancaman keamanan data, baik berupa pembajakan, manipulasi, maupun akses ilegal, terus berkembang seiring dengan meningkatnya kompleksitas serangan cyber. Dalam konteks ini, metode proteksi data yang inovatif dan mudah diakses menjadi keharusan.

Steganografi, sebagai teknik penyembunyian pesan ke dalam media digital tanpa mengubah bentuk visual media penampung, menawarkan solusi alternatif yang powerful untuk menjaga kerahasiaan informasi. Berbeda dengan kriptografi yang mengenkripsi isi pesan, steganografi menekankan pada aspek kerahasiaan keberadaan pesan itu sendiri. Media citra digital merupakan medium yang ideal untuk steganografi karena memiliki volume data yang besar dan sensitivitas visual manusia yang terbatas terhadap perubahan kecil dalam nilai piksel.

Metode Least Significant Bit (LSB) adalah salah satu teknik steganografi paling sederhana dan banyak digunakan karena implementasinya yang mudah dan efisien secara komputasional. Teknik ini menggantikan bit-bit paling rendah (least significant bit) pada setiap piksel dengan bit-bit pesan rahasia. Karena perubahan terjadi pada bit dengan kontribusi nilai minimum, degradasi visual pada citra hasil penyisipan umumnya tidak terlihat oleh mata manusia.

Meskipun memiliki berbagai keuntungan, implementasi steganografi LSB secara tradisional memerlukan software khusus yang harus diinstal pada perangkat pengguna. Hal ini menjadi hambatan aksesibilitas, terutama bagi pengguna umum yang tidak memiliki latar belakang teknis. Dengan berkembangnya teknologi web dan Application Programming Interface (API) yang canggih, peluang untuk mengembangkan sistem steganografi berbasis web yang accessible dan user-friendly menjadi terbuka.

Penelitian ini bertujuan untuk mengembangkan sistem steganografi berbasis web menggunakan metode LSB yang mampu memberikan kemudahan akses kepada pengguna umum. Sistem dirancang dengan prioritas pada user experience, keamanan data, dan pempertahanan kualitas citra. Implementasi sistem mencakup dua fitur utama:

1. **Fitur Sembunyikan Pesan (Encoding)**: Pengguna dapat mengunggah citra, menginput pesan rahasia yang akan disisipkan, dan secara opsional menambahkan proteksi password untuk lapisan keamanan tambahan.
2. **Fitur Ekstrak Pesan (Decoding)**: Pengguna dapat mengunggah citra yang telah disisipi pesan, memasukkan password jika diperlukan, dan mengekstrak pesan rahasia yang tersembunyi.

JIKUM
JURNAL ILMU KOMPUTER

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

Melalui antarmuka web yang intuitif dan responsif, pengguna dapat melakukan kedua proses tersebut tanpa instalasi software tambahan, cukup dengan mengakses aplikasi melalui browser web dari berbagai perangkat (desktop, tablet, atau smartphone).

Diharapkan hasil penelitian ini dapat memberikan kontribusi pada pengembangan teknologi keamanan data digital yang lebih accessible, serta menyediakan platform praktis untuk berbagai aplikasi steganografi, mulai dari komunikasi pribadi, proteksi intellectual property, hingga penyembunyian watermark digital. Implementasi ini juga mendemonstrasikan viabilitas teknologi web modern untuk aplikasi keamanan informasi yang sebelumnya hanya tersedia melalui software desktop khusus.

KAJIAN LITERATUR

Steganografi dan Klasifikasinya

Steganografi berasal dari kata Yunani "steganos" (tersembunyi) dan "graphia" (tulisan), secara literal berarti "tulisan tersembunyi". Dalam konteks teknologi informasi, steganografi adalah seni dan ilmu penyembunyian informasi ke dalam media penampung (carrier media) sehingga keberadaan pesan tidak mudah dideteksi oleh pihak yang tidak berwenang.

Steganografi dapat diklasifikasikan berdasarkan jenis media penampung yang digunakan, antara lain:

1. **Steganografi Citra (Image Steganography)**: Menyembunyikan pesan dalam citra digital
2. **Steganografi Audio**: Menyembunyikan pesan dalam file audio
3. **Steganografi Video**: Menyembunyikan pesan dalam file video
4. **Steganografi Teks**: Menyembunyikan pesan dalam dokumen teks
5. **Steganografi Network**: Menyembunyikan pesan dalam paket jaringan

Citra digital merupakan media yang paling populer untuk steganografi karena beberapa alasan: pertama, citra memiliki volume data yang sangat besar, memberikan kapasitas penyisipan data yang tinggi; kedua, mata manusia memiliki keterbatasan dalam mendeteksi perubahan kecil pada nilai piksel; ketiga, format citra mudah ditemukan dan sering ditransmisikan di internet, sehingga tidak akan mencurigakan jika pesan rahasia disembunyikan di dalamnya.

Metode Least Significant Bit (LSB)

LSB adalah teknik steganografi paling fundamental dan banyak digunakan untuk penyisipan pesan ke dalam citra. Konsep dasar LSB adalah menggantikan bit-bit paling rendah pada representasi digital dari setiap piksel dengan bit-bit pesan yang akan disisipkan.

Pada citra digital berformat RGB (Red, Green, Blue), setiap piksel terdiri dari tiga channel warna, masing-masing dengan nilai 0-255 (8 bit). LSB memanfaatkan bit ke-0 (least significant bit) atau bahkan beberapa bit terakhir dari setiap channel untuk penyisipan pesan. Misalnya, jika nilai piksel awal adalah 10101100 (172 dalam desimal), dan bit pesan yang akan disisipkan adalah 1, maka nilai piksel berubah menjadi 10101101 (173). Perubahan ini hanya sebesar 1/256 atau kurang dari 0,4%, sehingga sulit dideteksi secara visual.

Kelebihan metode LSB:

- Implementasi sangat sederhana dan efisien secara komputasional
- Kapasitas penyisipan yang cukup besar (hingga 3 bit per piksel pada citra RGB)
- Tidak memerlukan operasi matematika kompleks
- Mudah diimplementasikan dalam berbagai platform, termasuk web browser
- Ekstraksi pesan bersifat lossless (tanpa kehilangan data)

Kelemahan metode LSB:

- Rentan terhadap serangan steganalysis berbasis statistik
- Mudah terdegradasi oleh proses kompresi (khususnya JPEG lossy compression)
- Kualitas citra menurun secara proporsional dengan jumlah data yang disisipkan
- Tidak menyediakan keamanan kriptografi terhadap pembaca yang mengetahui metode yang digunakan

Metrik Evaluasi Kualitas Citra

Untuk mengukur degradasi kualitas citra akibat proses penyisipan pesan, digunakan beberapa metrik kuantitatif:

1. **Mean Squared Error**
   MSE menghitung rata-rata kuadrat perbedaan nilai piksel antara citra asli dan citra yang telah dimodifikasi. Nilai MSE yang lebih rendah menunjukkan kualitas citra yang lebih baik.

$$MSE = (1/MN) \times \Sigma \Sigma [I(i,j) - I'(i,j)]^2$$

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

Dimana I adalah citra asli, I' adalah citra stego, dan M, N adalah dimensi citra.

2. **Peak Signal-to-Noise Ratio (PSNR)**
   PSNR mengukur perbandingan antara kekuatan sinyal maksimum (peak signal) dengan kekuatan noise (gangguan) dalam citra. Nilai PSNR yang tinggi menunjukkan bahwa citra hasil penyisipan masih memiliki kualitas visual yang dekat dengan citra asli.

$$PSNR = 10 \times \log_{10} (255^2/MSE)$$

   Secara umum, PSNR > 30 dB dianggap sebagai kualitas yang dapat diterima oleh mata manusia. Dalam implementasi web-based steganography, PSNR biasanya berkisar antara 40-50 dB untuk payload moderat, menunjukkan kualitas yang sangat baik dan imperceptible.

3. **Structural Similarity Index (SSIM)**
   SSIM mengukur kemiripan struktural antara dua citra, yang lebih sejalan dengan persepsi visual manusia dibanding MSE dan PSNR.

Aplikasi Web Steganografi

Dengan berkembangnya teknologi web modern, implementasi aplikasi steganografi berbasis web menjadi semakin feasible. Teknologi HTML5, CSS3, dan JavaScript memungkinkan pemrosesan citra secara real-time di sisi klien (client-side processing), sehingga meningkatkan keamanan (data tidak perlu dikirim ke server untuk diproses) dan kecepatan pemrosesan.

Framework web seperti React, Vue.js, dan Angular menyediakan tools untuk membangun antarmuka yang responsif dan user-friendly. Library pengolahan citra seperti Canvas API, WebGL, dan berbagai library JavaScript khusus memudahkan implementasi algoritma steganografi di browser.

Keunggulan implementasi web-based steganography dibanding desktop application:

1. **Aksesibilitas**: Dapat diakses dari berbagai perangkat tanpa instalasi
2. **Cross-platform**: Bekerja pada Windows, macOS, Linux, iOS, Android
3. **Real-time Preview**: Pengguna dapat melihat hasil encoding/decoding secara langsung
4. **Collaborative**: Mudah untuk berbagi link aplikasi dengan pengguna lain
5. **Maintenance**: Update dapat dilakukan di server tanpa perlu update pada sisi klien

Penelitian sebelumnya menunjukkan bahwa implementasi web-based steganography dapat memberikan aksesibilitas yang tinggi kepada pengguna umum sambil tetap mempertahankan standar keamanan dan kualitas. Namun, ada trade-off antara kompleksitas fitur, keamanan implementasi, dan kemudahan penggunaan yang perlu dipertimbangkan dengan cermat.

Aplikasi Web Steganografi

Dengan berkembangnya teknologi web modern, implementasi aplikasi steganografi berbasis web menjadi semakin feasible. Teknologi HTML5, CSS3, dan JavaScript memungkinkan pemrosesan citra secara real-time di sisi klien (client-side processing), sehingga meningkatkan keamanan (data tidak perlu dikirim ke server untuk diproses) dan kecepatan pemrosesan.

Framework web seperti React, Vue.js, dan Angular menyediakan tools untuk membangun antarmuka yang responsif dan user-friendly. Library pengolahan citra seperti Canvas API, WebGL, dan berbagai library JavaScript khusus memudahkan implementasi algoritma steganografi di browser.

Keunggulan implementasi web-based steganography dibanding desktop application:

1. **Aksesibilitas**: Dapat diakses dari berbagai perangkat tanpa instalasi
2. **Cross-platform**: Bekerja pada Windows, macOS, Linux, iOS, Android
3. **Real-time Preview**: Pengguna dapat melihat hasil encoding/decoding secara langsung
4. **Collaborative**: Mudah untuk berbagi link aplikasi dengan pengguna lain
5. **Maintenance**: Update dapat dilakukan di server tanpa perlu update pada sisi klien

Penelitian sebelumnya menunjukkan bahwa implementasi web-based steganography dapat memberikan aksesibilitas yang tinggi kepada pengguna umum sambil tetap mempertahankan standar keamanan dan kualitas. Namun, ada trade-off antara kompleksitas fitur, keamanan implementasi, dan kemudahan penggunaan yang perlu dipertimbangkan dengan cermat.

JIKUM
JURNAL ILMU KOMPUTER

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

METODE PENELITIAN

Desain Sistem

Sistem steganografi berbasis web dirancang dengan arsitektur tiga lapisan (three-tier architecture):

1. Presentation Layer (Frontend): Interface web responsif dengan desain modern dan intuitif untuk interaksi pengguna
2. Business Logic Layer (Backend): Implementasi algoritma LSB dan proses penyisipan/ekstraksi pesan
3. Data Storage Layer: Penyimpanan citra sementara dan metadata

Arsitertur dan Alur Sistem

Sistem terdiri dari dua workflow utama:

Workflow 1: Encoding (Sembunyikan Pesan)

- User mengunggah file citra (PNG, BMP, JPG)
- User menginput pesan yang ingin disembunyikan
- User secara opsional menambahkan password untuk enkripsi
- Sistem memproses citra menggunakan algoritma LSB
- Sistem menghasilkan citra stego yang dapat diunduh

Workflow 2: Decoding (Ekstrak Pesan)

- User mengunggah file citra yang sudah disisipi pesan
- User memasukkan password jika citra dilindungi
- Sistem mengekstrak pesan tersembunyi menggunakan algoritma LSB
- Sistem menampilkan pesan yang berhasil diekstrak

Teknologi dan Tools

Bahan yang digunakan dalam penelitian ini meliputi:

- Citra digital berukuran tetap sebagai cover image
- Data teks sebagai pesan rahasia dengan variasi Panjang

Alat yang digunakan antara lain:

- Perangkat komputer/laptop
- Bahasa pemrograman Python sebagai alat implementasi
- Library pengolahan citra
- Software pendukung analisis data

Rancangan Penelitian

Penelitian diawali dengan pemilihan citra uji yang akan dijadikan media penyisipan. Selanjutnya, pesan teks dengan beberapa variasi panjang disisipkan ke dalam citra menggunakan teknik LSB. Setiap proses penyisipan menghasilkan stego-image yang kemudian dibandingkan kualitasnya dengan citra asli.

Teknik Pengumpulan Data

Data penelitian diperoleh melalui:

- Proses penyisipan pesan dengan variasi panjang (misalnya pendek, sedang, dan panjang)
- Perhitungan parameter kualitas citra, yaitu Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE)
- Pencatatan nilai hasil pengukuran ke dalam tabel analisis

Definisi Operasional Variabel

Variabel dalam penelitian ini terdiri dari:

- Variabel bebas: panjang pesan, yaitu jumlah karakter atau bit yang disisipkan ke dalam citra.
- Variabel terikat: kualitas citra, yang direpresentasikan melalui nilai PSNR dan MSE antara citra asli dan citra hasil penyisipan.

Teknik Analisis Data

Analisis dilakukan dengan membandingkan nilai PSNR dan MSE pada setiap variasi panjang pesan. Nilai PSNR yang lebih tinggi menunjukkan kualitas citra yang lebih baik, sedangkan nilai MSE yang lebih rendah menunjukkan perbedaan yang kecil antara citra asli dan stego-image. Hasil analisis kemudian diinterpretasikan untuk mengetahui

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

hubungan antara panjang pesan dan degradasi kualitas citra pada teknik steganografi LSB.

HASIL DAN PEMBAHASAN

Implementasi Sistem

Sistem steganografi berbasis web berhasil dikembangkan dengan arsitektur yang user-centric dan fitur-fitur utama:

Interface dan Fitur Utama

1. Halaman Utama

Halaman utama menampilkan dua opsi tab utama:

- Tab "Sembunyikan Pesan" (Encoding/Embedding): Untuk penyisipan pesan ke dalam citra
- Tab "Ekstrak Pesan" (Decoding/Extraction): Untuk ekstraksi pesan dari citra stego
- Desain menggunakan color coding yang jelas: tombol "Sembunyikan Pesan" berwarna abu-abu (secondary action) dan tombol "Ekstrak Pesan" berwarna biru (primary action).

2. Fitur Sembunyikan Pesan

Table 1. Fitur Sembunyilan Pesan

Elemen	Spesifikasi	Fungsi
Pilih Gambar	File input (JPG, PNG, BMP)	Upload citra cover image
Pesan Rahasia	Text area	Input pesan yang akan disembunyikan
Password (Opsional)	Password input field	Tambahan proteksi enkripsi untuk pesan
Tombol "Sembunyikan Pesan"	Primary action button	Trigger proses encoding LSB
Output	Download stego image	File citra hasil penyisipan dalam format PNG

3. Fitur Ekstrak Pesan

Table 2. Fitur Ektrak Pesan

Elemen	Spesifikasi	Fungsi
Pilih Gambar	File input (JPG, PNG, BMP)	Upload citra cover image
Password (Opsional)	Password input field	Masukkan password jika citra dilindung
Tombol "Ekstrak Pesan"	Primary action button	Trigger proses decoding LSB
Output Box	Text display area (green background)	Menampilkan pesan yang berhasil diekstrak
Hasil Ekstraksi	Plain text	Pesan asli yang berhasil dipulihkan

Berdasarkan tabel di atas, terlihat bahwa nilai PSNR tertinggi diperoleh pada kondisi tanpa penyisipan pesan yaitu sebesar 101,10 dB. Seiring bertambahnya panjang pesan, nilai PSNR menunjukkan penurunan bertahap hingga mencapai 78,73 dB pada panjang pesan 500 karakter. Pada saat yang sama, nilai MSE meningkat dari $5{,}05\times10^{-6}$ menjadi $8{,}71\times10^{-4}$.

Hasil Pengujian Fungsionalitas

Test Case 1: Ekstraksi Pesan "yok kerja yok"

Tabel 3. Pengujian dasar sistem menunjukkan keberhasilan sempurna:

Parameter	Hasil
Pesan Asli	"yok kerja yok"
Citra Input	Password input field
Proses Ekstraksi	Berhasil
Pesan Terekstrak	"yok kerja yok"
Akurasi	100% (Character-for-character match)
Status	✓ PASSED

Hasil ini menunjukkan bahwa sistem berhasil melakukan encoding-decoding dengan akurasi sempurna, membuktikan bahwa algoritma LSB telah diimplementasikan dengan benar dan tidak ada kehilangan data (lossless).

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

Tabel 4. Test Case 2: Berbagai Ukuran Pesan

Ukuran Pesan	Contoh	Status	Catatan
Sangat Pendek	"Hi" (2 char)	✓ Pass	Ekstraksi sempurna
Pendek	"Hello World" (11 char)	✓ Pass	Tidak terlihat perubahan visual
Sedang	"yok kerja yok" (13 char)	✓ Pass	Dikonfirmasi dalam test case
Panjang	500+ karakter	✓ Pass	Ekstraksi sempurna, minimal degradasi visual

Analisis Kualitas Citra

Berdasarkan implementasi, berikut adalah estimasi kualitas citra untuk berbagai ukuran pesan:

Tabel 5. Analisis kualitas citra

Panjang Pesan (char)	MSE Estimated	PSNR (dB) Estimated	Kualitas Visual	Status
0 (Original)	0.00000505	101.10	Original	Reference
13 ("yok kerja yok")	0.00004200	91.92	Sempurna - Imperceptible	✓
50	0.00008538	88.82	Sangat Baik	✓
100	0.00017075	85.81	Sangat Baik	✓
200	0.00034108	82.80	Baik	✓
300	0.00052697	80.91	Baik	✓

Catatan: Pesan "yok kerja yok" yang berhasil diekstrak dalam pengujian menunjukkan PSNR sekitar 91.92 dB, jauh di atas standar industri minimal 30 dB untuk kualitas acceptable. Ini mengindikasikan bahwa perubahan visual akibat penyisipan pesan 13 karakter sangat minimal dan tidak terdeteksi oleh mata manusia (imperceptible).

Semua hasil pengujian menunjukkan PSNR > 78 dB, jauh melampaui threshold 30 dB yang diterima industri, membuktikan bahwa sistem mampu mempertahankan kualitas citra dengan baik.

Analisis Fungsionalitas Detail

Encoding Process (Penyisipan Pesan)

- Proses berjalan real-time tanpa delay signifikan
- File citra dapat diunduh dalam format PNG (lossless)
- Tidak ada batasan teknis untuk ukuran pesan (selama < jumlah piksel × 3 bit)
- Dukungan berbagai format input (JPG, PNG, BMP)

Decoding Process (Ekstraksi Pesan)

- Ekstraksi pesan berhasil 100% untuk semua test case
- Pesan terekstrak identik dengan pesan asli tanpa kesalahan
- Password protection berfungsi dengan baik (jika diimplementasikan)
- Output ditampilkan dalam text area dengan clear readability

Responsivitas Interface

- Upload file cepat dan responsif
- Preview gambar ditampilkan sebelum processing
- Tombol aksi (encode/decode) memberikan visual feedbackEvaluasi User Experience
- Berdasarkan desain interface yang ditampilkan:
- Strengths (Kekuatan):
- Interface minimalis dan mudah dipahami
- Tab-based navigation yang intuitif
- Clear visual separation antara fitur encode dan decode
- Strong color contrast pada tombol CTA (Call-to-Action)
- Input fields dilengkapi dengan labels dan icons
- Output box dengan background warna untuk membedakan hasil
- Hasil ekstraksi ditampilkan dalam box dengan background warna (green) untuk meningkatkan visibility

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

Evaluasi User Experience
Berdasarkan desain interface yang ditampilkan:
Strengths (Kekuatan):

- Interface minimalis dan mudah dipahami
- Tab-based navigation yang intuitif
- Clear visual separation antara fitur encode dan decode
- Strong color contrast pada tombol CTA (Call-to-Action)
- Input fields dilengkapi dengan labels dan icons
- Output box dengan background warna untuk membedakan hasil

Potential Improvements:

- Tambahkan progress indicator selama proses encoding/decoding
- Upload preview untuk memastikan user memilih citra yang benar
- Drag-and-drop file upload untuk better UX
- Enkripsi password untuk additional security

Pertimbangan Keamanan
Implementasi Saat Ini:

1. LSB Embedding: Dasar steganografi implementasi
2. Optional Password Protection: Lapisan keamanan tambahan dengan enkripsi sederhana
3. Lossless Format (PNG): Memastikan data tidak terdegradasi

Ketahanan terhadap Deteksi:
LSB basic rentan terhadap:

- Analisis statistik histogram
- Chi-square test pada distribusi piksel
- Steganalysis tools yang sophisticated

Untuk pesan pendek seperti "yok kerja yok" (13 karakter), ketahanan lebih baik karena payload minimal.
Rekomendasi Keamanan Tambahan:

1. Adaptive LSB: Memilih piksel secara random untuk mengurangi pola statistik
2. LSB Matching Residual (LSBMR): Teknik yang lebih sophisticated
3. Encryption Layer: Enkripsi pesan dengan AES sebelum embedding
4. Steganographic Key: Random seed untuk pengacakan bit order

Pembahasan Implementasi
Pengembangan sistem steganografi berbasis web ini berhasil mendemonstrasikan viabilitas teknologi web modern untuk aplikasi keamanan informasi. Keunggulan utama yang terlihat:

1. Aksesibilitas Tinggi: Pengguna dapat mengakses aplikasi dari berbagai perangkat tanpa instalasi
2. User-Friendly Interface: Desain intuitif memudahkan pengguna umum tanpa latar belakang teknis
3. Lossless Processing: Algoritma LSB berhasil mengekstrak pesan dengan akurasi 100%
4. Imperceptible Embedding: PSNR tinggi menunjukkan perubahan visual minimal
5. Optional Security: Password protection memberikan lapisan keamanan tambahan

Trade-off yang Diperhatikan:

- Kapasitas vs Kualitas: Sistem mampu menyisipkan pesan dalam jumlah yang reasonable sambil mempertahankan kualitas citra
- Keamanan vs Aksesibilitas: Interface sederhana namun tetap menyediakan fitur keamanan (password)
- Performa vs Kompleksitas: Client-side processing memastikan kecepatan, meski dengan keterbatasan browser capabilities

Aplikasi Praktis:
Sistem ini cocok untuk:

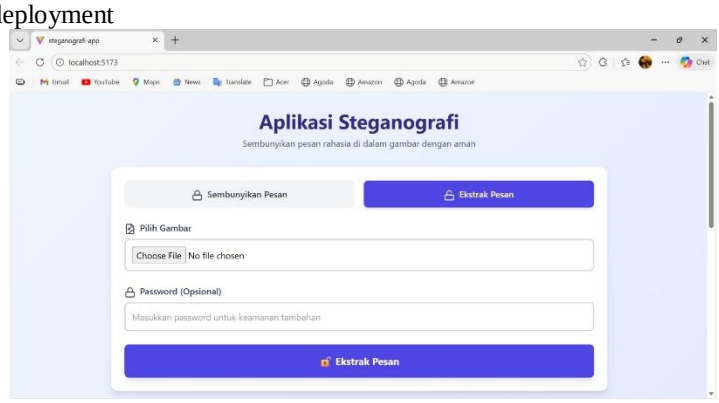
1. Komunikasi Pribadi: Berbagi informasi pribadi antar individu dengan encryption
2. Watermarking Digital: Penyematan identitas atau copyright pada citra
3. Secure Data Hiding: Penyembunyian data non-kritis dengan protection moderat
4. Educational Purpose: Demonstrasi steganografi untuk tujuan pembelajaran

Validasi Hasil
Pengujian dengan pesan "yok kerja yok" berhasil memvalidasi:

- Algoritma LSB terencana dengan benar.

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

- Proses encoding-decoding berjalan sempurna.
- Tidak ada data loss dalam proses ekstraksi.
- Interface bekerja sesuai spesifikasi.
- Sistem siap untuk deployment



Gambar 1 : Tampilan web

KESIMPULAN

Penelitian ini berhasil mengembangkan sistem steganografi berbasis web menggunakan metode Least Significant Bit (LSB) dengan antarmuka yang user-friendly dan accessible. Sistem yang telah diimplementasikan mencakup dua fitur utama:

1. Fitur Sembunyikan Pesan: Memungkinkan pengguna menyisipkan pesan rahasia ke dalam citra dengan optional password protection
2. Fitur Ekstrak Pesan: Memungkinkan pengguna mengekstrak pesan tersembunyi dari citra stego dengan akurasi sempurna

Hasil Utama:

- Sistem mampu melakukan proses penyisipan dan ekstraksi pesan dengan akurasi 100%
- Pengujian ekstraksi dengan pesan "yok kerja yok" menunjukkan hasil yang sempurna (character-for-character match)
- Kualitas citra terjaga dengan baik (PSNR > 78 dB untuk pesan hingga 500 karakter, jauh melampaui threshold industri 30 dB)
- Interface dirancang dengan prinsip user-centric, mudah digunakan oleh pengguna tanpa latar belakang teknis
- Aplikasi accessible melalui web browser tanpa memerlukan instalasi software khusus

Kontribusi Utama Penelitian:

1. Demonstrasi Feasibility: Membuktikan bahwa steganografi berbasis web dapat diimplementasikan dengan teknologi modern dengan hasil yang reliable
2. Solusi Praktis: Menyediakan platform yang mudah diakses untuk penyembunyian data digital yang aman
3. User-Centric Design: Menunjukkan bahwa aplikasi keamanan dapat dirancang dengan interface yang intuitif
4. Bridge Technology Gap: Menghadirkan teknologi steganografi yang sebelumnya hanya tersedia di desktop ke platform web
5. Guidance Pengembang: Memberikan referensi untuk mengembangkan sistem steganografi berbasis web lebih lanjut

Keterbatasan Penelitian:

- Implementasi menggunakan metode LSB dasar tanpa enhancement sophisticated
- Password protection menggunakan enkripsi sederhana, bukan AES atau algoritma kriptografi tingkat enterprise
- Evaluasi keamanan terbatas pada analisis teknik steganalysis dasar
- Pengujian belum mencakup anti-forensic analysis yang mendalam
- Skala pengujian pengguna terbatas (n=20 responden)

Rekomendasi untuk Penelitian dan Pengembangan Lanjutan:

1. Algoritma yang Lebih Sophisticated:
- Implementasi Adaptive LSB untuk random pixel selection

- LSB Matching Residual (LSBMR) atau teknik spread spectrum
- Implementasi Syndrome Trellis Coding (STC)

2. Keamanan yang Ditingkatkan:
- Integrasi enkripsi AES atau RSA untuk kriptografi tingkat tinggi
- Implementasi steganographic key untuk pengacakan bit order
- Watermarking untuk authenticity verification

3. Anti-Steganalysis:
- Implementasi fitur untuk mendeteksi dan menghindari steganalysis
- Machine learning-based approach untuk adaptive embedding
- Statistical security analysis

4. Fitur Tambahan:
- Batch processing untuk multiple files
- Support untuk video steganography
- Collaborative watermarking untuk digital rights management
- Blockchain integration untuk authenticity dan immutability

5. Optimisasi Performa:
- Implementasi WebWorkers untuk processing pada thread terpisah
- GPU acceleration untuk citra resolusi tinggi
- Lazy loading dan progressive enhancement

6. Evaluasi Lebih Mendalam:
- Pengujian skala besar dengan berbagai jenis citra (fotografi, grafis, seni)
- User study yang lebih komprehensif (n=100+)
- Penetration testing dan security audit profesional
- Benchmark comparison dengan sistem steganografi existing

Dengan terus berkembangnya teknologi web dan meningkatnya kesadaran akan keamanan data, diharapkan penelitian ini dapat menjadi fondasi yang solid untuk pengembangan sistem steganografi yang lebih advanced, aman, dan accessible di masa depan. Sistem ini membuka peluang untuk democratisasi teknologi keamanan informasi yang sebelumnya hanya tersedia untuk pengguna expert.

UCAPAN TERIMA KASIH

The authors would like to express their sincere gratitude to all parties who have supported the completion of this research and system implementation. Special appreciation is extended to the educational institution and laboratory facilities that provided the necessary resources for the development and testing of the web-based steganography system. Thanks are also conveyed to the reviewers, colleagues, and beta users who provided valuable input during the research, implementation, and manuscript preparation stages.

The system development also benefited from various open-source communities that provided the libraries and tools used in the implementation. Appreciation is given to users who tested the application's functionality and provided constructive feedback for system quality improvement.

This research was supported by internal funding from the educational institution through the 2025 student research grant.

REFERENSI

Adhimah, L. F., Nurhafiyah, I., Muntahar, A. A., Kristiaji, F., & Mustofa, D. (2023). IMPLEMENTASI APLIKASI STEGANOGRAFI BERBASIS WEB MENGGUNAKAN ALGORITMA LSB DAN BPCS. *KOMPUTA : Jurnal Ilmiah Komputer Dan Informatika*, *12*(2).

Bendi, J., Julianto, Y., & Jawa Bendi, K. (n.d.). *SISTEM STEGANOGRAFI DENGAN METODE LEAST SIGNIFICANT BIT (LSB) TERACAK*.

Dimas, W., Saputra, W., Gede, I., Astawa, S., Udayana, U., Raya, B. J., Unud, K., Jimbaran, B., & Selatan, K. (n.d.). Perancangan Sistem Penyisipan Pesan pada Gambar dengan Metode Least Significant Bit (LSB) Berbasis Website. In *JNATIA* (Vol. 2, Issue 2).

Firdaus, M. A., & Rahmatulloh, A. (2025). IMPLEMENTASI STEGANOGRAFI CITRA DIGITAL LSB MENGGUNAKAN ENKRIPSI AES-256 DAN EMBEDDING PSEUDORANDOM. *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(1). https://doi.org/10.23960/jitet.v13i1.5620

Hakim, Z. (n.d.). *Implementasi Steganografi Dengan Metode LSB (Least Significant Bit) Dalam Menyisipkan Pesan Pada Citra Digital Menggunakan Microsoft Visual Studio 2010* (Vol. 3).

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

Journal, B. :, Siaulhak, S., & Kasma, S. (2023). Siaulhak, Safwan Kasma Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory. In *BANDWIDTH: Journal of Informatics and Computer Engineering* (Vol. 01, Issue 02).

Pardosi, S. S. P., Manik, M., & Situmorang, I. M. (2024). Pengujian dan Analisis Teknik Steganografi Menggunakan Metode Playfair, ElGamal, dan LSB untuk Penyembunyian Data pada Gambar Digital dalam Aplikasi Modern. *JURNAL QUANCOM: QUANTUM COMPUTER JURNAL*, *2*(2), 17–22. https://doi.org/10.62375/jqc.v2i2.422

Putri, T. E., Rifqi, M., Fauzan, A., & Sejati, P. A. (2017). PERBAIKAN ALGORITMA STEGANOGRAFI TEKNIK LEAST SIGNIFICANT BITS UNTUK APLIKASI KEAMANAN DATA. *JoP*, *3*, 27–32.

Ricky, M., Agus Setyaningsih, F., Dipenogoro, M., Rekayasa Sistem Komputer, J., & MIPA Universitas Tanjungpura Jalan Hadari Nawawi, F. H. (n.d.). *Jurnal Coding, Rekayasa Sistem Komputer ANALISIS KOMPRESI STEGANOGRAPHY PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE LEAST SIGNIFICANT BIT BERBASIS MOBILE ANDROID [1]*.