Jurnal Elektronik Ilmu Komputer Udayana
Volume 14, No 4. May 2026

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Penyisipan Pesan Rahasia pada Citra Digital dengan Metode Steganografi dan Algoritma *Least Significant Bit* (LSB)

Made Dhandy Satria Mahagangga[a1], Luh Gede Astuti[a2], Luh Arida Ayu Rahning Putri[3], I Gede Surya Rahayuda[4]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]dhandysatria19@gmail.com
[2]lg.astuti@unud.ac.id
[3]rahningputri@unud.ac.id
[4]igedesuryarahayuda@unud.ac.id

Abstract

This study discusses the implementation of the Least Significant Bit (LSB) steganography method to insert secret messages into digital images by adding the Caesar Cipher algorithm as an additional security layer. The secret message is first encrypted using the Caesar Cipher before being embedded into the least significant bit of digital image pixels. This approach ensures that the message is not only visually hidden but also protected in terms of content. The system is developed as a web-based application using HTML, CSS, and JavaScript, enabling users to perform message insertion and extraction directly through a browser without installing additional software. Image quality evaluation is conducted using Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The experimental results show that the LSB method produces low MSE values and high PSNR values, indicating minimal visual distortion. The combination of LSB steganography and Caesar Cipher encryption proves effective in enhancing information security on digital image media.

Keywords: *Steganography, Least Significant Bit (LSB), Caesar Cipher, Digital Image, Information Security, PSNR, MSE*

1. Pendahuluan

Kemajuan teknologi informasi telah mendorong peningkatan aktivitas pertukaran data melalui berbagai media digital. Informasi yang dikirimkan secara elektronik memiliki risiko keamanan yang cukup tinggi karena dapat diakses, dimodifikasi, maupun disalahgunakan oleh pihak yang tidak memiliki hak akses. Oleh sebab itu, diperlukan mekanisme pengamanan yang mampu menjaga kerahasiaan data selama proses penyimpanan maupun pengiriman informasi. Salah satu teknik yang dapat digunakan adalah steganografi, yaitu metode penyembunyian pesan ke dalam suatu media seperti citra digital, audio, atau video sehingga keberadaan pesan tidak mudah diketahui oleh pihak lain.

Metode Least Significant Bit (LSB) merupakan teknik steganografi yang banyak digunakan karena proses implementasinya relatif sederhana serta mampu mempertahankan kualitas visual media penampung. Teknik ini bekerja dengan memanfaatkan bit yang memiliki bobot nilai paling rendah pada setiap piksel citra sebagai lokasi penyisipan data rahasia. Namun, beberapa penelitian terdahulu yang menerapkan metode LSB masih berfokus pada keberhasilan proses penyisipan dan ekstraksi pesan serta kualitas citra hasil steganografi. Apabila pesan berhasil diekstraksi dari citra stego, isi pesan dapat langsung dibaca karena tidak memperoleh perlindungan tambahan pada tingkat isi informasi. Kondisi ini menunjukkan bahwa metode LSB memiliki keterbatasan dalam menjaga kerahasiaan pesan ketika proses ekstraksi berhasil dilakukan oleh pihak yang tidak berwenang.

Untuk mengatasi keterbatasan tersebut, penelitian ini mengombinasikan metode LSB dengan algoritma Caesar Cipher sebagai lapisan keamanan tambahan. Caesar Cipher dipilih karena memiliki mekanisme enkripsi yang sederhana, ringan, dan mudah diimplementasikan pada

p-ISSN: 2301-5373
e-ISSN: 2654-5101

aplikasi berbasis web tanpa memerlukan sumber daya komputasi yang besar. Pada penelitian ini, pesan rahasia terlebih dahulu dienkripsi menggunakan Caesar Cipher sebelum disisipkan ke dalam citra digital menggunakan metode LSB. Dengan demikian, apabila pesan berhasil diekstraksi oleh pihak yang tidak berwenang, informasi yang diperoleh masih berupa ciphertext dan tidak dapat langsung dipahami tanpa mengetahui kunci yang digunakan. Penelitian ini bertujuan untuk mengimplementasikan kombinasi kedua metode tersebut serta mengevaluasi keberhasilannya dalam menjaga kualitas citra dan meningkatkan keamanan informasi pada media citra digital.

2. Tinjauan Pustaka

2.1. Steganografi

Steganografi merupakan teknik pengamanan informasi yang dilakukan dengan cara menyisipkan data rahasia ke dalam suatu media digital tanpa mengubah tampilan media tersebut secara mencolok. Tujuan utama dari steganografi adalah menyembunyikan keberadaan pesan sehingga pihak lain tidak menyadari bahwa media yang digunakan mengandung informasi tambahan. Dalam perkembangannya, steganografi sering dikombinasikan dengan teknik kriptografi untuk meningkatkan tingkat keamanan data yang disembunyikan.

Menurut Alanzy *et al* (2023), steganografi modern mampu meningkatkan keamanan data melalui kombinasi teknik penyisipan dan algoritma kriptografi sehingga pesan menjadi lebih sulit dideteksi oleh pihak yang tidak berwenang.

2.2. Citra Digital

Citra digital adalah representasi gambar dalam bentuk data numerik yang dapat diproses oleh komputer. Sebuah citra tersusun atas kumpulan piksel yang masing-masing memiliki nilai warna tertentu. Pada citra RGB, setiap piksel terdiri dari komponen merah (Red), hijau (Green), dan biru (Blue) yang memiliki rentang nilai antara 0 hingga 255. Banyaknya jumlah piksel pada citra digital memungkinkan media tersebut digunakan sebagai wadah penyisipan pesan rahasia tanpa menimbulkan perubahan visual yang mudah terlihat.

Penelitian oleh Rustad *et al* (2022) mengembangkan metode steganografi LSB terbalik menggunakan pola adaptif untuk meningkatkan imperceptibility, menunjukkan bahwa pemilihan pola yang optimal dalam penyisipan data dapat meminimalkan distorsi pada citra stego.

2.3. Least Significant Bit (LSB)

Least Significant Bit (LSB) merupakan metode penyisipan data yang memanfaatkan bit dengan tingkat signifikansi paling rendah pada setiap piksel citra digital. Proses penyisipan dilakukan dengan mengganti nilai bit tersebut menggunakan bit pesan yang akan disembunyikan. Karena perubahan hanya terjadi pada bit dengan kontribusi nilai yang sangat kecil, kualitas visual citra umumnya tetap terjaga. Oleh karena itu, metode LSB banyak digunakan dalam penelitian steganografi karena menawarkan kapasitas penyisipan yang cukup besar dengan tingkat distorsi citra yang rendah.

Penelitian oleh Veriarinal dan Wanandi (2024) menunjukkan bahwa algoritma LSB mampu melakukan proses encoding dan decoding pesan dengan baik serta menghasilkan kualitas citra yang tetap terjaga berdasarkan parameter MSE dan PSNR.

2.4. Caesar Cipher

Caesar Cipher termasuk salah satu algoritma kriptografi klasik yang menerapkan teknik pergeseran karakter berdasarkan nilai kunci tertentu. Setiap huruf pada pesan asli akan digeser sejumlah posisi sesuai nilai kunci yang digunakan sehingga menghasilkan pesan terenkripsi. Meskipun metode ini tergolong sederhana, Caesar Cipher masih sering dimanfaatkan sebagai media pembelajaran konsep dasar kriptografi maupun sebagai lapisan keamanan tambahan ketika dikombinasikan dengan metode pengamanan lainnya.

Rumus enkripsi Caesar Cipher :

$$C = (P + K) \, mod \, 26$$

Rumus dekripsi Caesar Cipher :

$$P = (C - K) \, mod \, 26$$

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Sebagai contoh, jika plaintext “HELLO” dienkripsi menggunakan *shift key* 3, maka ciphertext yang dihasilkan adalah “KHOOR”.
Penelitian oleh Purnamasari (2021) menunjukkan bahwa Caesar Cipher memiliki kecepatan enkripsi yang tinggi dan mudah diimplementasikan, namun tingkat keamanannya masih rendah sehingga umumnya dikombinasikan dengan metode lain seperti steganografi untuk meningkatkan keamanan pesan.

2.5. Mean Squared Error (MSE)

Mean Squared Error (MSE) merupakan parameter yang digunakan untuk mengukur tingkat perbedaan antara citra asli dengan citra hasil penyisipan pesan. Nilai MSE diperoleh dari rata-rata kuadrat selisih nilai piksel pada kedua citra tersebut. Semakin kecil nilai MSE yang dihasilkan, semakin kecil pula perubahan yang terjadi akibat proses steganografi sehingga kualitas citra hasil penyisipan dapat dikatakan semakin baik.

Rumus MSE :

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2$$

Penelitian oleh Bai *et al* (2023) dalam jurnal Sensors mengaplikasikan MSE untuk mengevaluasi akurasi prediksi model dalam algoritma steganografi pada citra inframerah. Temuan penelitian memperlihatkan bahwa model yang diajukan memiliki performa yang lebih baik ditinjau dari nilai MSE yang lebih rendah dibandingkan metode terdahulu, sehingga menghasilkan citra prediksi dengan tingkat kesalahan yang lebih kecil.

2.6. Peak Signal-to-Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) digunakan sebagai parameter evaluasi untuk mengetahui tingkat kualitas citra hasil steganografi dibandingkan dengan citra asli. Nilai PSNR dinyatakan dalam satuan desibel (dB). Semakin tinggi nilai PSNR yang diperoleh, semakin kecil tingkat distorsi yang terjadi pada citra hasil penyisipan. Oleh karena itu, nilai PSNR sering digunakan bersama MSE untuk menilai keberhasilan proses steganografi.
Rumus PSNR :

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

Penelitian oleh Bai *et al* (2023) dalam jurnal Sensors menggunakan PSNR untuk mengevaluasi kualitas citra hasil steganografi. Temuan penelitian menunjukkan bahwa metode yang diusulkan menghasilkan nilai PSNR yang tinggi, sehingga citra hasil steganografi tetap mempertahankan kualitas visualnya dan memiliki perbedaan yang sangat minim dibandingkan dengan citra asli.

3. Metode Penelitian

3.1 Sumber dan Jenis data

Internet dan koleksi pribadi peneliti berfungsi sebagai sumber data penelitian. Untuk mendapatkan berbagai gambar dengan kualitas yang beragam, gambar digital diperoleh dari situs web Pexels, Freepik, dan Pinterest, selain foto pribadi peneliti sendiri.

Data gambar digital dalam format PNG, JPG, dan JPEG, serta data teks berupa pesan rahasia yang akan disematkan ke dalam gambar digital, merupakan jenis data yang digunakan..

3.2 Metode Pengembangan Sistem

Pengembangan sistem pada penelitian ini menggunakan metode Prototype. Pendekatan ini dipilih karena memungkinkan peneliti membangun rancangan awal sistem yang dapat langsung diuji oleh pengguna. Melalui proses evaluasi yang dilakukan secara berulang, prototype dapat diperbaiki dan disesuaikan hingga memenuhi kebutuhan yang telah ditentukan. Dengan demikian, proses pengembangan sistem menjadi lebih fleksibel dan mampu menghasilkan aplikasi yang sesuai dengan tujuan penelitian.

Tahapan metode Prototype terdiri dari :

p-ISSN: 2301-5373
e-ISSN: 2654-5101

1. Analisis kebutuhan.
2. Perancangan sistem.
3. Pembangunan prototype.
4. Pengujian sistem.
5. Evaluasi sistem.

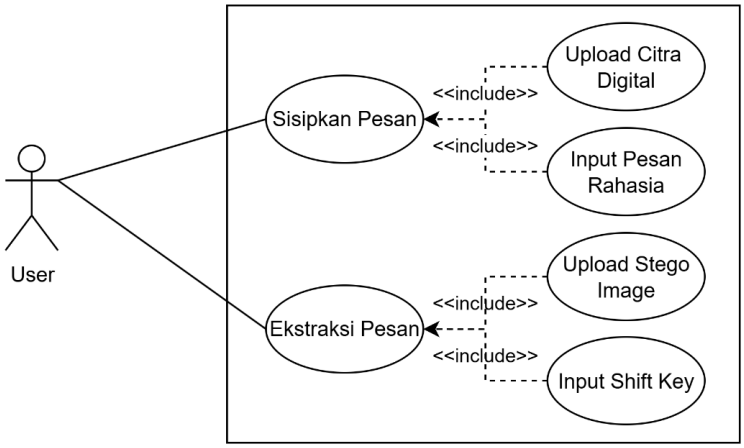
3.3 Analisis Kebutuhan Fungsional

Kebutuhan fungsional system terdiri dari :

1. Sistem dapat menerima input citra digital dari pengguna.
2. Sistem dapat menerima input pesan rahasia yang akan disisipkan ke dalam citra.
3. Sistem dapat menerima input *shift key* untuk proses Caesar Cipher.
4. Sistem dapat melakukan proses enkripsi pesan menggunakan algoritma Caesar Cipher.
5. Sistem dapat mengubah pesan terenkripsi ke dalam bentuk biner.
6. Sistem dapat melakukan proses penyisipan pesan menggunakan algoritma Least Significant Bit (LSB).
7. Sistem dapat menghasilkan *stego image* sebagai hasil dari penyisipan pesan.
8. Sistem dapat melakukan proses ekstraksi pesan dari *stego image* menggunakan algoritma Least Significant Bit (LSB).
9. Sistem dapat melakukan proses dekripsi pesan menggunakan Caesar Cipher.
10. Sistem dapat menampilkan pesan hasil ekstraksi.
11. Sistem dapat menghitung nilai Mean Squared Error (MSE).
12. Sistem dapat menghitung nilai Peak Signal-to-Noise Ratio (PSNR).
13. Sistem dapat menampilkan hasil evaluasi kualitas citra berdasarkan nilai MSE dan PSNR.
14. Sistem dapat mengunduh *stego image* ke perangkat.

3.4 Use Case Diagram Sistem

Use Case Diagram digunakan untuk menggambarkan hubungan antara pengguna dengan fitur-fitur yang tersedia pada aplikasi. Dalam penelitian ini hanya terdapat satu aktor, yaitu pengguna (user), yang berinteraksi langsung dengan sistem. Pengguna memiliki akses untuk melakukan proses unggah citra, memasukkan pesan rahasia, menjalankan proses penyisipan pesan, melakukan ekstraksi data, serta melihat hasil evaluasi kualitas citra yang dihasilkan oleh sistem..

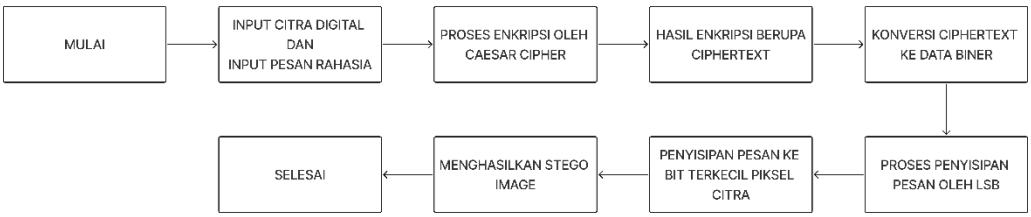


Gambar 1. Use Case Diagram Sistem

Pada penelitian ini, sistem hanya melibatkan satu aktor yaitu user, karena seluruh proses pengolahan data dilakukan secara client-side melalui browser tanpa melibatkan administrator maupun server backend. User berperan sebagai pengguna utama yang melakukan proses penyisipan pesan rahasia dan proses ekstraksi pesan dari stego image. Seluruh proses kriptografi dan steganografi dilakukan secara otomatis oleh sistem setelah user memberikan input yang dibutuhkan.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

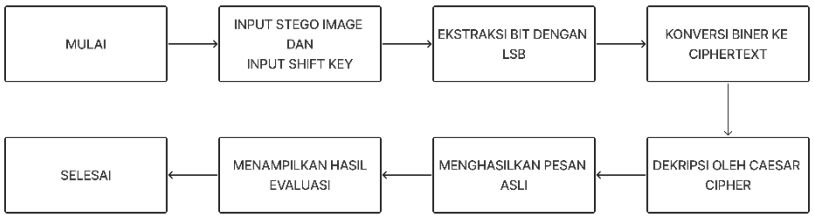
3.5 Alur Penyisipan Pesan



Gambar 2. Alur Penyisipan Pesan

Alur penyisipan pesan dimulai ketika pengguna memasukkan citra digital dan pesan rahasia yang akan disembunyikan ke dalam sistem. Selanjutnya, sistem melakukan proses enkripsi pesan menggunakan algoritma Caesar Cipher sehingga menghasilkan ciphertext. Ciphertext yang dihasilkan kemudian dikonversi ke dalam bentuk data biner agar dapat diproses menggunakan metode Least Significant Bit (LSB). Setelah proses konversi selesai, sistem melakukan penyisipan bit-bit pesan ke dalam bit paling kecil pada setiap piksel citra digital menggunakan metode LSB. Proses ini dilakukan secara bertahap hingga seluruh pesan berhasil disisipkan ke dalam citra. Setelah proses penyisipan selesai dilakukan, sistem menghasilkan stego image yang telah mengandung pesan rahasia dengan kualitas visual yang hampir sama seperti citra asli.

3.6 Alur Ekstraksi Pesan



Gambar 3. Alur Ekstraksi Pesan

Alur ekstraksi pesan dimulai ketika pengguna mengunggah stego image dan memasukkan shift key yang sesuai ke dalam sistem. Selanjutnya, sistem melakukan proses ekstraksi bit pesan dari bit paling kecil pada setiap piksel citra menggunakan metode Least Significant Bit (LSB). Bit-bit hasil ekstraksi kemudian dikonversi kembali dari bentuk biner menjadi ciphertext. Setelah ciphertext berhasil diperoleh, sistem melakukan proses dekripsi menggunakan algoritma Caesar Cipher dengan shift key yang telah dimasukkan sebelumnya. Hasil dari proses dekripsi tersebut berupa pesan asli yang sebelumnya telah disisipkan ke dalam citra digital. Setelah seluruh proses selesai dilakukan, sistem menampilkan hasil evaluasi dan pesan rahasia berhasil dikembalikan ke bentuk semula.

4. Hasil Dan Pembahasan

Sistem steganografi berhasil diimplementasikan dalam bentuk website menggunakan HTML, CSS, dan JavaScript. Sistem memanfaatkan FileReader API dan Canvas API untuk membaca serta mengolah data piksel citra secara client-side.

Sistem mampu melakukan proses :

1. Enkripsi pesan menggunakan Caesar Cipher.

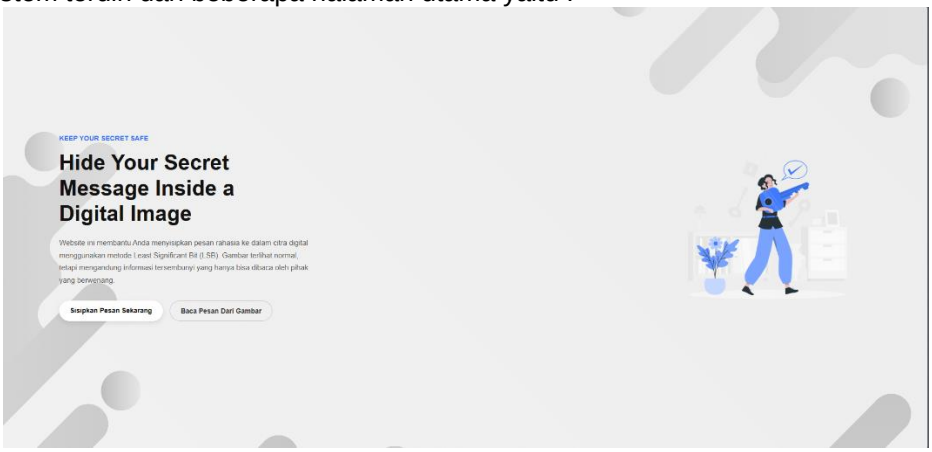
p-ISSN: 2301-5373
e-ISSN: 2654-5101

2. Penyisipan pesan menggunakan Least Significant Bit.
3. Ekstraksi pesan.
4. Dekripsi pesan
5. Perhitungan MSE dan PSNR.

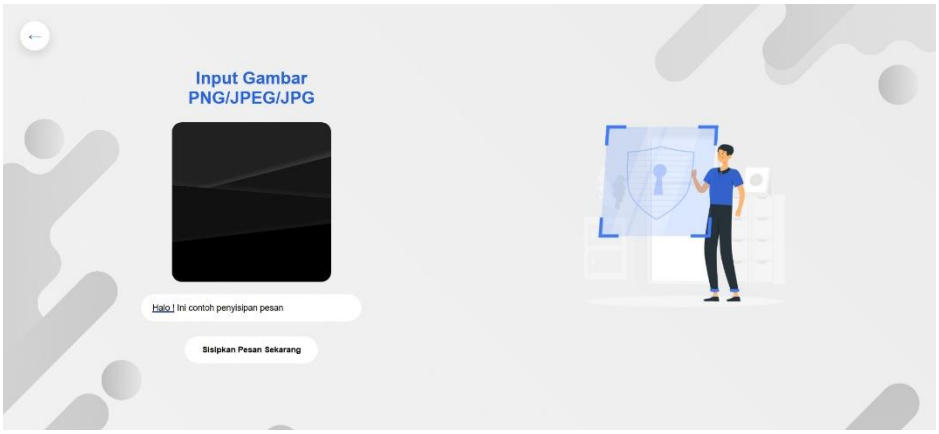
Pengujian dilakukan menggunakan citra dengan format PNG, JPG, dan JPEG serta panjang pesan 100 dan 200 karakter.
Dari hasil pengujian dapat diketahui bahwa informasi yang disisipkan ke dalam citra dapat diekstraksi kembali secara lengkap tanpa terjadi perubahan isi pesan. Kualitas citra hasil steganografi juga tetap terpelihara, sebagaimana ditunjukkan oleh tingkat kesalahan yang rendah (MSE) dan rasio kualitas citra yang tinggi (PSNR).

4.1 Implementasi Sistem

Implementasi sistem dilakukan dengan membangun aplikasi steganografi berbasis website menggunakan HTML, CSS, dan JavaScript. Sistem dirancang agar seluruh proses pengolahan data dilakukan secara client-side melalui browser tanpa memerlukan server backend. Sistem terdiri dari beberapa halaman utama yaitu :

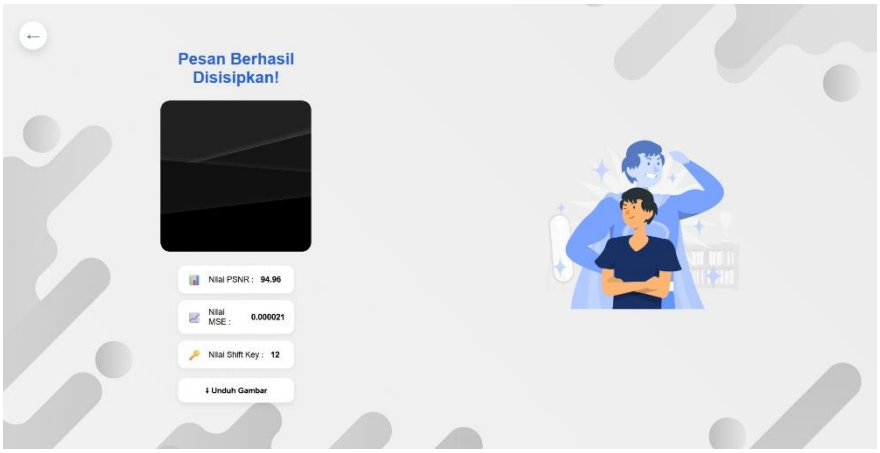


Gambar 4. Halaman Utama

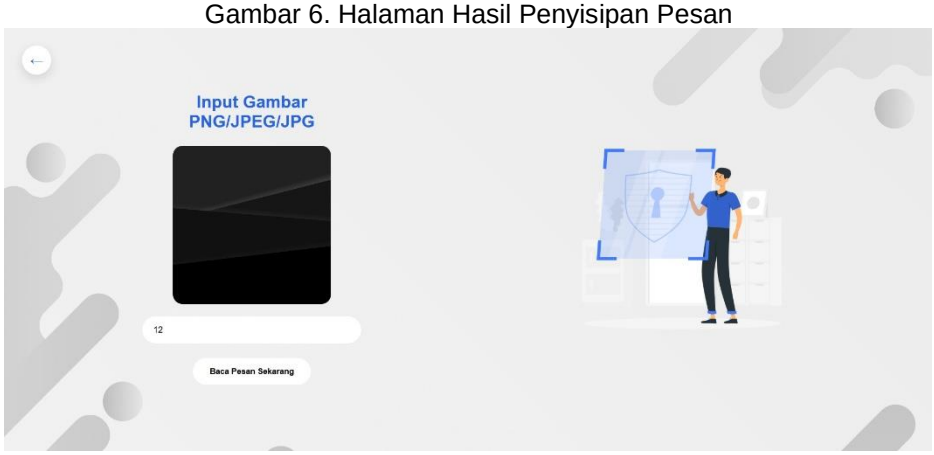


Gambar 5. Halaman Penyisipan Pesan

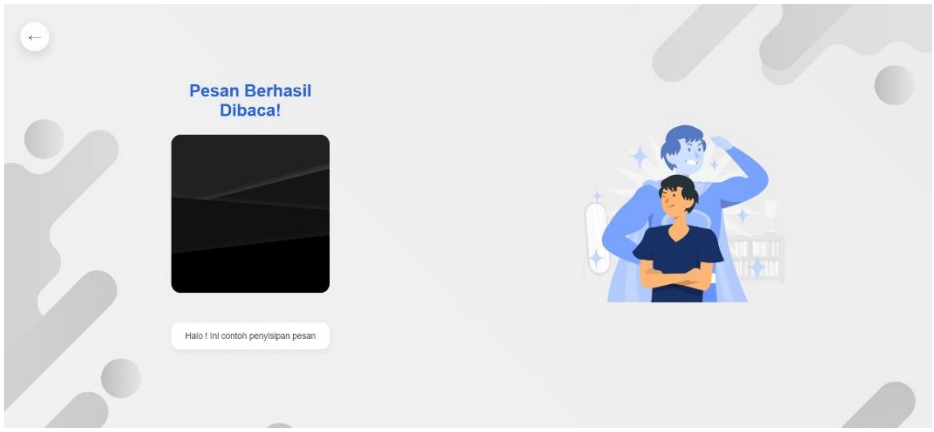
p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 6. Halaman Hasil Penyisipan Pesan



Gambar 7. Halaman Ekstraksi Pesan



Gambar 8. Halaman Hasil Ekstraksi Pesan

4.2 Pengujian Black Box

Untuk memastikan kualitas dan kinerja sistem, dilakukan pengujian **Black Box** terhadap seluruh fitur yang tersedia pada aplikasi steganografi. Metode ini digunakan untuk mengevaluasi kesesuaian fungsi sistem dengan kebutuhan yang telah ditentukan pada tahap perancangan. Pengujian dilakukan dengan memberikan berbagai skenario masukan dan mengamati keluaran yang dihasilkan oleh sistem. Dengan pendekatan ini, aspek yang dinilai berfokus pada fungsionalitas sistem tanpa memperhatikan implementasi atau struktur kode program yang mendasarinya.

Penggunaan metode Black Box Testing bertujuan untuk mengevaluasi aspek fungsional sistem melalui pengamatan terhadap kesesuaian antara keluaran aktual dan keluaran yang diharapkan. Berdasarkan penelitian Huda dkk. (2022), metode ini memiliki kemampuan yang

p-ISSN: 2301-5373
e-ISSN: 2654-5101

baik dalam mengidentifikasi kesalahan validasi input sekaligus memastikan bahwa seluruh fungsi sistem telah berjalan sesuai dengan kebutuhan dan spesifikasi pengguna.

Tabel 1. Hasil Black Box Testing

No	Fitur yang Diuji	Hasil Pengujian	Status
1	Input Citra Digital	Sistem berhasil menerima dan menampilkan citra digital dari pengguna	Berhasil
2	Input Pesan Rahasia	Sistem berhasil menerima pesan rahasia yang akan disisipkan ke dalam citra	Berhasil
3	Input Shift Key	Sistem berhasil menerima shift key untuk proses enkripsi dan dekripsi	Berhasil
4	Enkripsi Caesar Cipher	Sistem berhasil melakukan proses enkripsi pesan menggunakan algoritma Caesar Cipher	Berhasil
5	Konversi Pesan ke Bentuk Biner	Sistem berhasil mengubah pesan terenkripsi ke dalam bentuk biner	Berhasil
6	Penyisipan Pesan Menggunakan LSB	Sistem berhasil melakukan proses penyisipan pesan menggunakan algoritma Least Significant Bit (LSB)	Berhasil
7	Generate Stego Image	Sistem berhasil menghasilkan stego image sebagai hasil penyisipan pesan	Berhasil
8	Ekstraksi Pesan Menggunakan LSB	Sistem berhasil mengekstraksi pesan dari stego image menggunakan algoritma Least Significant Bit (LSB)	Berhasil
9	Dekripsi Caesar Cipher	Sistem berhasil melakukan proses dekripsi pesan menggunakan Caesar Cipher	Berhasil
10	Menampilkan Pesan Hasil Ekstraksi	Sistem berhasil menampilkan pesan hasil ekstraksi kepada pengguna	Berhasil
11	Perhitungan Nilai MSE	Sistem berhasil menghitung nilai Mean Squared Error (MSE)	Berhasil
12	Perhitungan Nilai PSNR	Sistem berhasil menghitung nilai Peak Signal-to-Noise Ratio	Berhasil

p-ISSN: 2301-5373
e-ISSN: 2654-5101

No	Fitur yang Diuji	Hasil Pengujian	Status
		(PSNR)	
13	Menampilkan Hasil Evaluasi Kualitas Citra	Sistem berhasil menampilkan hasil evaluasi kualitas citra berdasarkan nilai MSE dan PSNR	Berhasil
14	Mengunduh Stego Image	File berhasil diunduh	Berhasil

Berdasarkan hasil pengujian Black Box, seluruh fitur pada sistem steganografi berbasis website berhasil berjalan sesuai dengan fungsi yang diharapkan.

4.3 Pengujian Penyisipan dan Ekstraksi Pesan

Untuk menilai kemampuan sistem, dilakukan serangkaian pengujian menggunakan kombinasi ukuran citra digital dan panjang pesan yang berbeda-beda. Dari hasil pengujian tersebut dapat diketahui bahwa mekanisme penyisipan maupun pengambilan kembali pesan berjalan dengan sukses, sehingga pesan dapat diproses dengan benar pada seluruh kondisi pengujian yang telah ditetapkan.

Tabel 2. Hasil Pengujian Penyisipan dan Ekstraksi Pesan

No	Format Gambar	Resolusi Citra	Panjang Pesan	Hasil Embedding	Hasil Extraction
1	PNG	256 x 256 512 x 512 1920 x 1080	100 dan 200 Karakter	Berhasil	Berhasil
2	JPG	256 x 256 512 x 512 1920 x 1080	100 dan 200 Karakter	Berhasil	Berhasil
3	JPEG	256 x 256 512 x 512 1920 x 1080	100 dan 200 Karakter	Berhasil	Berhasil

4.4 Pengujian MSE dan PSNR

Untuk mengetahui tingkat kualitas citra yang dihasilkan, dilakukan pengujian menggunakan parameter Mean Squared Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) sebagai indikator tingkat perbedaan dan kualitas citra.

Tabel 2 Hasil Pengujian MSE dan PSNR

Resolusi	Pengulangan	Panjang Pesan	Rata-rata MSE	Rata-rata PSNR
256x256	5x	100 Karakter	0.001687	75.86 dB
		200 Karakter	0.003149	73.15 dB
512x512	5x	100 Karakter	0.000403	82.08 dB
		200 Karakter	0.000799	79.11 dB
1920x1080	5x	100 Karakter	0.000799	91.16 dB
		200 Karakter	0.000100	88.13 dB

5. Kesimpulan dan Saran

5.1 Kesimpulan

Hasil penelitian menunjukkan bahwa implementasi sistem steganografi berbasis website dengan memanfaatkan metode Least Significant Bit (LSB) dan algoritma Caesar Cipher telah

p-ISSN: 2301-5373
e-ISSN: 2654-5101

berjalan dengan baik. Sistem yang dibangun mampu menyembunyikan pesan rahasia ke dalam citra digital serta mengembalikannya melalui proses ekstraksi dengan tingkat keberhasilan yang tinggi. Kualitas citra setelah proses penyisipan tetap terjaga karena perbedaan antara citra asli dan citra stego sangat kecil, yang dibuktikan melalui nilai MSE yang rendah dan nilai PSNR yang tinggi. Selain menjaga kualitas media penyimpanan, penggunaan Caesar Cipher juga meningkatkan aspek keamanan data, sehingga pesan yang diperoleh dari hasil ekstraksi tidak dapat langsung dibaca tanpa mengetahui kunci pergeseran yang digunakan pada tahap enkripsi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa sistem steganografi berbasis web yang menerapkan metode Least Significant Bit (LSB) dan algoritma Caesar Cipher berhasil diimplementasikan sesuai dengan tujuan yang telah ditetapkan. Sistem mampu melakukan proses penyisipan dan ekstraksi pesan rahasia dengan baik tanpa menyebabkan penurunan kualitas visual citra yang signifikan. Kombinasi kedua metode tersebut memberikan lapisan keamanan tambahan yang cukup efektif dalam menjaga kerahasiaan informasi yang disembunyikan di dalam media citra digital.

Sebagai pengembangan pada penelitian selanjutnya, sistem dapat ditingkatkan dengan menerapkan algoritma kriptografi yang lebih kuat, seperti AES atau RSA, sehingga tingkat keamanan pesan menjadi lebih optimal. Selain itu, metode steganografi yang digunakan dapat dikembangkan dengan memanfaatkan teknik lain, seperti Discrete Cosine Transform (DCT) atau Discrete Wavelet Transform (DWT), untuk meningkatkan ketahanan sistem terhadap berbagai bentuk manipulasi maupun modifikasi citra. Pengembangan sistem ke platform mobile serta penambahan fitur keamanan, seperti perlindungan berbasis kata sandi, juga dapat dilakukan guna meningkatkan fleksibilitas penggunaan dan memperkuat keamanan sistem dalam berbagai kebutuhan pengamanan informasi digital.

Daftar Pustaka

[1]. Alanzy, M., Alomrani, R., Alqarni, B. & Almutairi, S., 2023. Image Steganography Using LSB and Hybrid Encryption Algorithms. Applied Sciences, 13(21), pp. 1–20.

[2] Bai, Y., Li, L., Lu, J., Zhang, S. & Chu, N., 2023. A Novel Steganography Method for Infrared Image Based on Smooth Wavelet Transform and Convolutional Neural Network. Sensors, 23(12), p. 5360.

[3] Huda, M. N., Burhan, M., Satibi, A., Pradita, H. A., Saifudin, A. & Kusyadi, I., 2022. Implementasi Black Box Testing pada Aplikasi Sistem Kasir dengan Menggunakan Teknik Equivalence Partitions. Jurnal Teknologi Sistem Informasi dan Aplikasi, 5(2), pp. 120–127.

[4] Rustad, S., Ignatius, R., Rosal, M. & Syukur, A., 2022. Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility. Journal of King Saud University - Computer and Information Sciences, 34(6), pp. 3559–3568.

[5] Veriarinal, V. & Wanandi, R., 2024. Implementasi Sistem Steganografi Citra dengan Metode Substitusi LSB (Least Significant Bit). Kohesi: Jurnal Multidisiplin Saintek, 2(11), pp. 10–20.

[6] Purnamasari, D. (2021). Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher untuk Keamanan Data Teks Menggunakan Python. Journal of Informatics Education, 4(1), 45–53.