JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Steganografi pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) dengan Pengamanan Pesan Menggunakan Kriptografi Sederhana

Mohammad Haykhal Nasution[1*], Nura Dara Anrilva[2], Nazwa Salsabilah[3], Shafa Adira Rizky[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]mohammad.230170166@mhs.unimal.ac.id, [2]nura.230170194@mhs.unimal.ac.id,
[3]nazwa.230170196@mhs.unimal.ac.id, [4]shafa.230170198@mhs.unimal.ac.id

ABSTRACT

Steganography is a technique used to conceal secret information within digital media in order to prevent unauthorized parties from detecting the existence of the message. One commonly used approach is the Least Significant Bit (LSB) *method due to its simplicity and high imperceptibility. However, if the hidden message is successfully extracted, the confidentiality of its content may still be at risk. Therefore, this research implements a digital image steganography system using the LSB method, in which the secret message is first encrypted using a simple encryption mechanism before the embedding process. The encrypted message is then embedded into a digital image by modifying the least significant bits of pixel values. The developed web-based application allows users to embed and extract secret messages effectively. The results show that the embedding and extraction processes are successfully performed, and the stego image does not exhibit noticeable visual differences compared to the original image. These results indicate that the proposed approach can conceal secret messages while maintaining acceptable visual quality of the image.*

Keywords:
Steganography, Least Significant Bit (LSB)*, Digital Image, Simple Encryption, Information Security*

PENDAHULUAN

Perkembangan teknologi digital yang semakin pesat turut meningkatkan risiko terhadap keamanan informasi, terutama dalam proses pertukaran informasi melalui jaringan terbuka. Informasi digital rentan terhadap penyadapan, pencurian, dan manipulasi oleh pihak yang tidak berwenang. Salah satu teknik yang digunakan untuk melindungi informasi adalah steganografi, yaitu metode penyembunyian pesan rahasia ke dalam media digital seperti citra sehingga keberadaan pesan tersebut sulit dideteksi secara visual maupun analitis (Fahmi et al., 2023; Krisna, I Gusti Ngurah Febri Ananda Karyawati, 2024).

*Least Significant Bit (*LSB) merupakan salah satu teknik steganografi yang paling umum digunakan karena kemudahannya dalam implementasi serta kemampuannya mempertahankan kualitas visual citra setelah proses penyisipan pesan (Fahmi et al., 2023). Metode ini bekerja dengan memodifikasi bit paling rendah pada nilai piksel citra untuk menyimpan pesan rahasia. Meskipun perubahan visual yang dihasilkan relatif kecil, pesan yang disisipkan tanpa pengamanan tambahan masih dapat dibaca secara langsung apabila proses ekstraksi berhasil dilakukan oleh pihak yang tidak berwenang. Hal ini menunjukkan bahwa steganografi saja belum cukup untuk menjamin kerahasiaan isi pesan secara menyeluruh (S & Hasanuddin, 2021).

Berdasarkan permasalahan tersebut, penelitian ini mengimplementasikan sistem steganografi citra digital menggunakan metode LSB dengan menerapkan enkripsi sederhana pada pesan rahasia sebelum proses penyisipan dilakukan. Pendekatan ini bertujuan untuk meningkatkan tingkat keamanan pesan, di mana pesan tidak hanya tersembunyi di dalam citra tetapi juga terlindungi dari akses tidak sah melalui proses enkripsi. Sistem yang dikembangkan diimplementasikan dalam bentuk aplikasi berbasis web yang mampu melakukan proses penyisipan dan ekstraksi pesan secara efektif serta mempertahankan kualitas visual citra stego yang dihasilkan. tidak menurunkan kualitas gambar secara signifikan.

KAJIAN LITERATUR

Steganografi Citra Digital

Steganografi adalah teknik yang bertujuan untuk menyembunyikan keberadaan pesan rahasia ke dalam media digital sehingga pihak lain tidak menyadari adanya pesan tersebut. Teknik ini berbeda dari kriptografi yang fokus pada pengacakan isi pesan, karena steganografi berfokus pada “penyamaran pesan” secara visual maupun struktural (Fahmi et al., 2023). Media yang umum digunakan dalam steganografi antara lain citra, audio, dan video, dimana citra digital sering dipilih karena memiliki kapasitas penyisipan data yang relatif besar dengan perubahan visual yang minimal.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

Metode *Least Significant Bit* (LSB)

LSB merupakan salah satu metode steganografi yang paling sederhana dan populer karena implementasinya yang mudah serta hasil yang relatif natural secara visual. Metode ini bekerja dengan cara mengganti bit paling rendah dari representasi biner nilai piksel dengan bit pesan. Teknik ini banyak digunakan dalam steganografi citra karena perubahan yang terjadi pada bit paling rendah tidak terlalu terlihat secara kasat mata (Krisna, I Gusti Ngurah Febri Ananda Karyawati, 2024).

Penelitian sebelumnya mengembangkan variasi metode LSB, termasuk modifikasi urutan bit atau kombinasi dengan kompresi, guna meningkatkan kapasitas penyisipan dan keamanan pesan (S & Hasanuddin, 2021) Namun, tantangan utama LSB tetap terletak pada potensi ekstraksi pesan tanpa otorisasi apabila metode penyisipan diketahui oleh pihak lain.

Pengamanan Pesan melalui Enkripsi

Meskipun steganografi dapat menyembunyikan keberadaan pesan, isi pesan yang disisipkan masih berpotensi bocor apabila berhasil diekstraksi oleh pihak yang tidak berwenang. Oleh karena itu, pengamanan tambahan berupa enkripsi pesan dilakukan sebelum proses penyisipan untuk menjaga kerahasiaan isi pesan. Penggunaan enkripsi sederhana seperti *Caesar cipher, XOR cipher*, atau algoritma ringan lainnya dapat meningkatkan keamanan tanpa menambah beban komputasi yang signifikan (Rahman et al., 2023).

Kombinasi Steganografi dan Kriptografi

Kombinasi steganografi dan kriptografi merupakan pendekatan yang banyak digunakan untuk meningkatkan keamanan informasi digital. Pada pendekatan ini, pesan rahasia terlebih dahulu dienkripsi menggunakan algoritma kriptografi, kemudian hasil enkripsi tersebut disisipkan ke dalam media citra menggunakan metode steganografi, seperti LSB. Penelitian oleh (Rahman et al., 2023) menunjukkan bahwa kombinasi teknik steganografi LSB dengan enkripsi multi-level dapat meningkatkan resistensi terhadap pengambilan pesan secara tidak sah, terutama ketika pesan tersebut disimpan dalam komponen bagian citra yang kurang terlihat.

Evaluasi Kualitas Citra Stego

Evaluasi kualitas citra stego merupakan tahap penting dalam penelitian steganografi citra digital untuk memastikan bahwa proses penyisipan pesan tidak menimbulkan perubahan visual yang signifikan pada citra. Pada penelitian steganografi, kualitas citra stego umumnya dapat dievaluasi menggunakan parameter kuantitatif seperti *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR), sebagaimana dilaporkan dalam beberapa penelitian sebelumnya.

Namun, pada penelitian ini evaluasi kualitas citra stego dilakukan secara kualitatif melalui pengamatan visual, dengan membandingkan citra asli dan citra stego secara langsung. Pengamatan difokuskan pada perubahan warna, tingkat kejernihan, serta detail visual citra setelah proses penyisipan pesan.

Berdasarkan hasil pengujian, citra stego yang dihasilkan tidak menunjukkan perbedaan visual yang signifikan dibandingkan dengan citra asli. Hal ini menunjukkan bahwa metode Least Significant Bit (LSB) mampu menyisipkan pesan rahasia dengan tetap menjaga kualitas visual citra sehingga perubahan yang terjadi sulit dideteksi secara kasat mata.

Studi Terkait Sistem Pengamanan Kombinasi

Beberapa penelitian modern menerapkan gabungan antara steganografi dan teknik pengamanan lainnya seperti metode enkripsi *AES*, kunci simetris, atau model hybrid untuk meningkatkan keamanan pesan secara keseluruhan tanpa mengorbankan kualitas citra (Aribowo et al., 2025; Patil & Sonaje, 2024). Pendekatan ini turut menunjukkan bahwa steganografi tidak berdiri sendiri, tetapi dapat ditingkatkan melalui integrasi teknik kriptografi sebagai *pre-processing* sebelum embedding.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan implementatif dengan pengujian fungsional dengan fokus pada implementasi dan pengujian sistem steganografi citra digital menggunakan metode LSB. Metode LSB dipilih karena memiliki tingkat imperceptibility yang tinggi serta mudah diimplementasikan pada citra digital berwarna (Singh & Sharma, 2022). Dalam penelitian ini, pesan rahasia terlebih dahulu dienkripsi secara sederhana sebelum proses penyisipan dilakukan untuk meningkatkan keamanan isi pesan, sebagaimana direkomendasikan dalam penelitian steganografi modern (Al-Dmour et al., 2023).

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

Data Penelitian

Data yang digunakan dalam penelitian ini terdiri dari:

1. Citra digital berwarna RGB berformat JPG dan PNG sebagai media penyisipan.
2. Pesan teks sebagai informasi rahasia.
3. Kunci enkripsi untuk proses kriptografi sederhana.

Output yang dihasilkan berupa citra stego dan pesan hasil ekstraksi.

Metode Kriptografi Sederhana

Pesan teks dienkripsi terlebih dahulu menggunakan kriptografi sederhana berbasis kunci sebelum proses steganografi. Proses ini bertujuan untuk memberikan lapisan keamanan tambahan sehingga pesan tidak dapat dipahami meskipun berhasil diekstraksi tanpa kunci yang benar.

Tahapan kriptografi meliputi:

1. Konversi pesan ke bentuk karakter ASCII.
2. Proses enkripsi menggunakan kunci.
3. Hasil enkripsi digunakan sebagai input steganografi.

Metode Steganografi LSB

Metode LSB digunakan dengan cara menyisipkan bit pesan terenkripsi ke dalam bit paling tidak signifikan dari nilai piksel citra digital. Penyisipan dilakukan pada kanal warna citra sehingga perubahan visual citra tetap minimal.
Langkah utama metode LSB:

1. Konversi pesan terenkripsi ke bentuk biner.
2. Modifikasi bit LSB piksel citra.
3. Pembentukan citra stego.

Alur Sistem

Sistem memiliki dua proses utama, yaitu penyisipan (*embedding*) dan ekstraksi (*extracting*).
Proses Penyisipan:

1. Input citra digital dan pesan.
2. Enkripsi pesan menggunakan kriptografi sederhana.
3. Penyisipan pesan terenkripsi menggunakan metode LSB.
4. Pembentukan citra stego.

Proses Ekstraksi:

1. Input citra stego.
2. Pembacaan bit LSB piksel citra.
3. Dekripsi pesan menggunakan kunci.
4. Penampilan pesan asli.

Implementasi Sistem

Sistem diimplementasikan dalam bentuk aplikasi web menggunakan HTML dan JavaScript. Pengolahan citra dilakukan melalui Canvas API, sedangkan proses kriptografi dan steganografi diimplementasikan menggunakan JavaScript. Aplikasi memungkinkan pengguna melakukan proses embedding dan extracting secara langsung melalui antarmuka web.

Metode Pengujian

Pengujian sistem dilakukan dengan:

1. Pengujian fungsional, untuk memastikan pesan dapat disisipkan dan diekstraksi dengan benar.
2. Pengujian kualitas citra, melalui pengamatan visual citra asli dan citra stego.
3. Pengujian keamanan, dengan memastikan pesan tidak dapat dibaca tanpa kunci yang sesuai.

Teknik Analisis

Hasil pengujian dianalisis secara deskriptif berdasarkan:

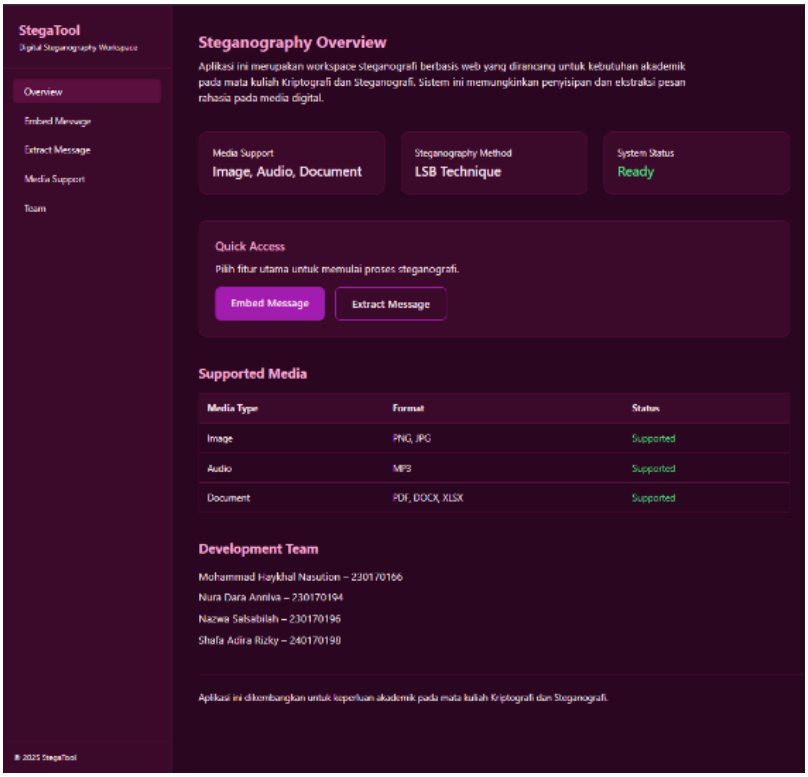
1. Keberhasilan proses penyisipan dan ekstraksi pesan.
2. Perubahan visual pada citra stego.
3. Keamanan pesan terhadap akses tanpa kunci.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

HASIL DAN PEMBAHASAN

Hasil Implementasi Sistem



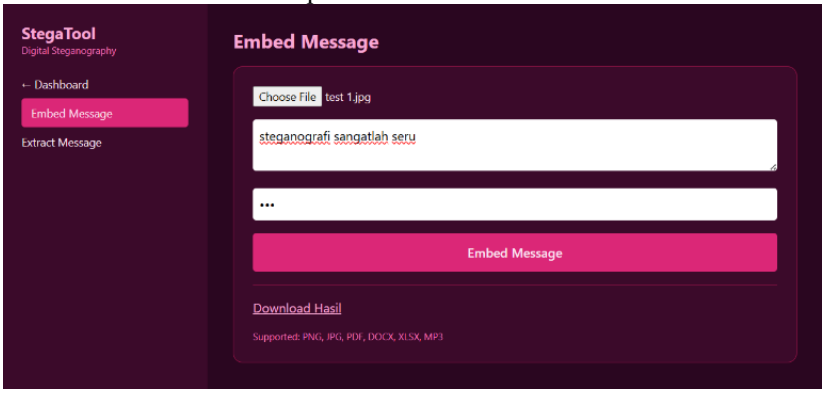
Gambar 1. Tampilan Dashboard Aplikasi

Gambar 1 menunjukkan tampilan dashboard utama aplikasi. Pada tampilan ini, pengguna disajikan dengan antarmuka sederhana yang menyediakan akses ke dua fungsi utama, yaitu proses penyisipan pesan *(embedding)* dan proses ekstraksi pesan *(extracting)*. Desain antarmuka dibuat intuitif agar pengguna dapat menjalankan proses steganografi tanpa memerlukan pemahaman teknis yang mendalam mengenai algoritma yang digunakan.

Dari hasil pengujian fungsional, aplikasi menerima input berupa citra digital berformat JPG dan PNG serta pesan teks sebagai informasi rahasia. Sistem juga menyediakan input kunci yang digunakan dalam proses enkripsi dan dekripsi pesan. Seluruh proses berjalan melalui peramban web tanpa memerlukan instalasi perangkat lunak tambahan, sehingga aplikasi bersifat portabel dan mudah diakses. Hal ini menunjukkan bahwa sistem yang dikembangkan telah memenuhi tujuan implementasi sebagai aplikasi steganografi berbasis web yang fungsional.

Proses Penyisipan Pesan

Proses penyisipan pesan merupakan tahap utama dalam sistem steganografi yang dikembangkan. Pada tahap ini, pesan rahasia dimasukkan oleh pengguna dan selanjutnya disisipkan ke dalam citra digital sehingga keberadaan pesan tidak dapat dikenali secara kasat mata. Proses ini diawali dengan pemilihan citra digital sebagai media penyisipan, diikuti dengan input pesan rahasia dan kunci enkripsi.



Gambar 2. Tampilan Form Penyisipan Pesan

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

Gambar 2 memperlihatkan tampilan antarmuka proses penyisipan pesan. Pada halaman ini, pengguna dapat memilih citra digital yang akan digunakan sebagai media penyisipan, memasukkan pesan teks yang bersifat rahasia dan kata kunci agar pesan terenkripsi. Setelah seluruh input diberikan, sistem akan memproses pesan dengan melakukan enkripsi sederhana sebelum pesan tersebut disisipkan ke dalam citra menggunakan metode LSB. Proses enkripsi sederhana pada pesan bertujuan untuk memberikan lapisan keamanan tambahan. Pesan yang telah dienkripsi akan berubah menjadi bentuk yang tidak dapat dipahami secara langsung, sehingga meskipun pesan berhasil diekstraksi oleh pihak yang tidak berwenang, isi pesan tetap tidak dapat dibaca tanpa kunci yang sesuai. Hasil enkripsi ini selanjutnya dikonversi ke dalam bentuk biner sebagai persiapan untuk proses penyisipan ke dalam citra.

Tahap selanjutnya adalah proses steganografi menggunakan metode Least Significant Bit (LSB). Pada tahap ini, bit-bit dari pesan terenkripsi disisipkan ke dalam bit paling tidak signifikan dari nilai piksel citra digital. Penyisipan dilakukan pada kanal warna citra sehingga perubahan nilai piksel yang terjadi sangat kecil dan tidak menimbulkan perbedaan visual yang signifikan. Setelah seluruh bit pesan berhasil disisipkan, sistem menghasilkan citra stego sebagai output dari proses embedding.

Hasil Citra Steganografi

Bagian ini membahas hasil citra digital setelah proses penyisipan pesan rahasia menggunakan LSB. Evaluasi dilakukan dengan membandingkan citra asli *(cover image)* dan citra hasil steganografi *(stego image)* secara visual untuk mengetahui sejauh mana proses penyisipan memengaruhi kualitas citra.

Gambar 3. Citra Asli

Gambar 3 menampilkan citra asli yang digunakan sebagai media penyisipan pesan. Citra ini merupakan citra berwarna RGB dengan format JPG yang dipilih sebagai cover image. Citra asli berfungsi sebagai acuan untuk menilai perubahan visual yang terjadi setelah proses steganografi dilakukan.

Gambar 4. Citra Stego

Gambar 4 menunjukkan citra stego yang dihasilkan setelah pesan rahasia terenkripsi disisipkan ke dalam citra menggunakan metode LSB. Secara visual, citra stego tampak serupa dengan citra asli dan tidak menunjukkan adanya perubahan mencolok. Hal ini disebabkan oleh metode LSB yang hanya memodifikasi bit paling tidak signifikan dari nilai piksel, sehingga perubahan yang terjadi sangat kecil dan sulit dideteksi oleh penglihatan manusia.

Berdasarkan hasil pengamatan visual, dapat disimpulkan bahwa proses steganografi yang diterapkan tidak menurunkan kualitas citra secara signifikan. Citra stego yang dihasilkan masih layak digunakan dan tidak menimbulkan

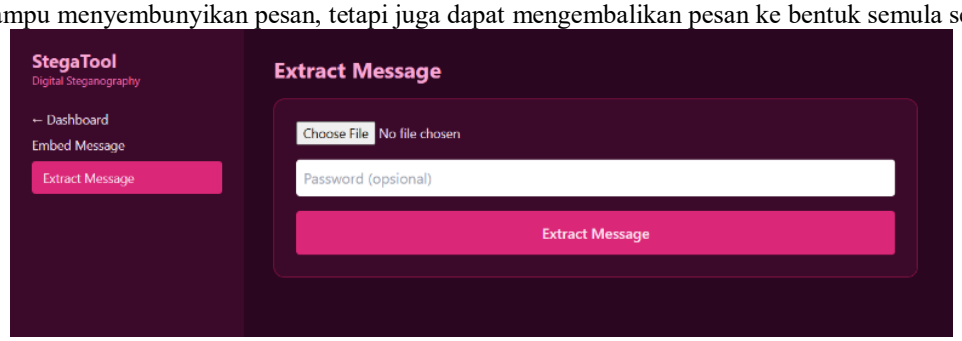
This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

kecurigaan secara visual. Dengan demikian, metode LSB yang digunakan dalam penelitian ini terbukti efektif dalam menyisipkan pesan rahasia sambil mempertahankan kualitas visual citra sebagai media penyisipan.

Proses Ekstraksi Pesan *(Extracting)*

Proses ekstraksi pesan merupakan tahap lanjutan dari sistem steganografi yang bertujuan untuk mengambil kembali pesan rahasia yang telah disisipkan ke dalam citra stego. Tahap ini penting untuk membuktikan bahwa sistem tidak hanya mampu menyembunyikan pesan, tetapi juga dapat mengembalikan pesan ke bentuk semula secara akurat.

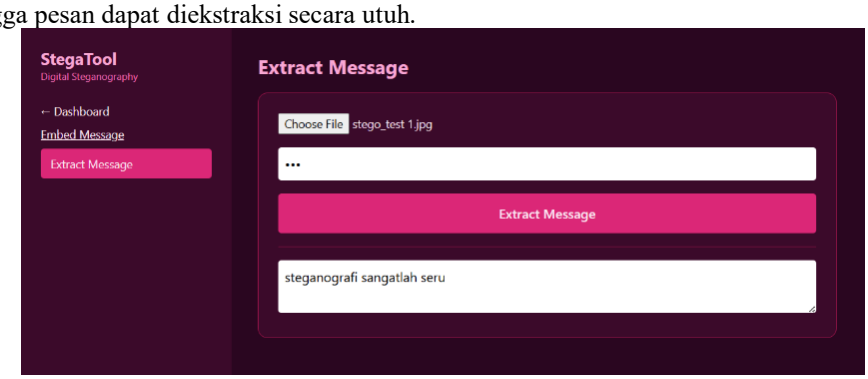


Gambar 5. Tampilan Form Ekstraksi Pesan

Gambar 5 menunjukkan tampilan antarmuka proses ekstraksi pesan pada aplikasi. Pada halaman ini, pengguna diminta untuk memasukkan citra stego yang sebelumnya dihasilkan dari proses penyisipan pesan. Selain itu, pengguna juga harus memasukkan kunci yang sama dengan kunci yang digunakan pada proses enkripsi saat penyisipan. Kesesuaian kunci menjadi faktor utama dalam keberhasilan proses dekripsi pesan.

Setelah citra stego dimasukkan, sistem melakukan pembacaan bit paling tidak signifikan (LSB) dari setiap piksel citra untuk mengekstraksi bit-bit pesan terenkripsi. Bit-bit tersebut kemudian disusun kembali menjadi data pesan terenkripsi.

Proses ini dilakukan secara berurutan sesuai dengan mekanisme penyisipan yang digunakan pada tahap embedding, sehingga pesan dapat diekstraksi secara utuh.



Gambar 6. Hasil pesan rahasia setelah proses ekstraksi berhasil dilakukan.

Tahap selanjutnya adalah proses dekripsi pesan menggunakan kunci yang diberikan oleh pengguna. Apabila kunci yang dimasukkan sesuai, sistem akan berhasil mengembalikan pesan ke bentuk teks aslinya. Gambar 6 memperlihatkan hasil pesan yang berhasil diekstraksi dan didekripsi. Pesan yang ditampilkan sama dengan pesan yang dimasukkan pada tahap penyisipan, yang menunjukkan bahwa proses ekstraksi dan dekripsi berjalan dengan benar. Berdasarkan hasil pengujian, sistem mampu mengekstraksi pesan secara akurat tanpa mengalami kehilangan atau perubahan isi pesan. Sebaliknya, apabila kunci yang dimasukkan tidak sesuai, pesan yang dihasilkan tidak dapat dibaca dengan benar. Hal ini membuktikan bahwa penerapan enkripsi sederhana pada pesan sebelum penyisipan memberikan kontribusi terhadap aspek keamanan sistem, karena pesan tidak dapat dipahami tanpa kunci yang tepat.

Dengan demikian, hasil proses ekstraksi pesan menunjukkan bahwa sistem steganografi yang dikembangkan telah berfungsi sesuai dengan perancangan. Keberhasilan ekstraksi dan dekripsi pesan menegaskan bahwa metode LSB yang diterapkan mampu menyimpan dan mengembalikan pesan rahasia secara efektif.

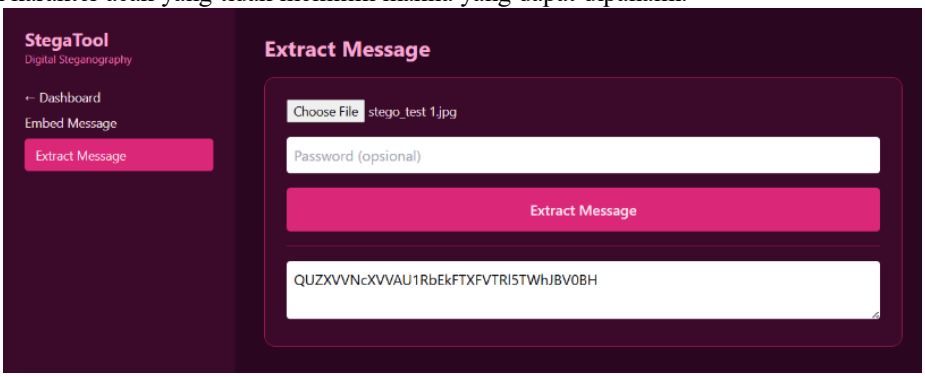
Pembahasan Keamanan Sistem

Berdasarkan hasil pengujian, pesan yang telah dienkripsi sebelum disisipkan ke dalam citra tidak dapat dipahami secara langsung tanpa memasukkan kunci yang sesuai. Hal ini terlihat dari perbedaan hasil ekstraksi ketika proses dekripsi dilakukan dengan dan tanpa kunci. Apabila kunci yang dimasukkan sesuai, sistem mampu mengembalikan

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

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

pesan ke bentuk teks aslinya. Sebaliknya, apabila kunci tidak dimasukkan atau tidak sesuai, pesan yang dihasilkan berupa rangkaian karakter acak yang tidak memiliki makna yang dapat dipahami.



Gambar 7. Hasil ekstraksi pesan tanpa memasukkan kunci yang sesuai

Kondisi tersebut ditunjukkan pada Gambar 7, di mana proses ekstraksi pesan dilakukan tanpa memasukkan kunci. Hasil ekstraksi yang ditampilkan berupa teks terenkripsi yang tidak dapat dibaca secara langsung. Hal ini menunjukkan bahwa meskipun proses ekstraksi bit pesan dari citra stego berhasil dilakukan, isi pesan tetap terlindungi karena tidak melalui proses dekripsi yang benar. Dengan demikian, enkripsi sederhana berfungsi sebagai lapisan keamanan tambahan terhadap isi pesan. Dari sisi steganografi, penggunaan metode *Least Significant Bit* (LSB) memberikan tingkat penyamaran yang baik terhadap keberadaan pesan rahasia. Modifikasi bit paling tidak signifikan pada nilai piksel citra tidak menimbulkan perubahan visual yang mencolok, sehingga citra stego sulit dibedakan dari citra asli secara kasat mata. Kondisi ini mengurangi kemungkinan pihak lain menyadari adanya informasi tersembunyi di dalam citra. Kombinasi antara steganografi dan enkripsi sederhana pada sistem ini menghasilkan dua lapisan keamanan, yaitu penyembunyian keberadaan pesan dan perlindungan terhadap isi pesan.

Secara keseluruhan, pembahasan keamanan sistem menunjukkan bahwa penerapan enkripsi sederhana sebelum proses steganografi mampu melindungi isi pesan meskipun proses ekstraksi berhasil dilakukan tanpa kunci yang benar. Hasil ini telah memenuhi tujuan penelitian, yaitu menghasilkan sistem steganografi citra digital yang fungsional, mudah digunakan, dan memiliki tingkat keamanan yang lebih baik dibandingkan sistem steganografi tanpa pengamanan pesan.

KESIMPULAN

Metode LSB yang digunakan dalam penelitian ini terbukti mampu menyisipkan pesan rahasia tanpa menimbulkan perubahan visual yang signifikan pada citra. Citra hasil steganografi secara kasat mata sulit dibedakan dari citra asli, sehingga metode ini efektif dalam menyembunyikan keberadaan pesan rahasia di dalam citra digital. Penerapan enkripsi sederhana sebelum proses penyisipan pesan memberikan lapisan keamanan tambahan terhadap isi pesan. Hasil pengujian menunjukkan bahwa pesan hanya dapat dikembalikan ke bentuk aslinya apabila kunci yang digunakan sesuai. Apabila kunci tidak dimasukkan atau tidak sesuai, pesan yang dihasilkan tidak dapat dipahami, sehingga isi pesan tetap terlindungi meskipun proses ekstraksi berhasil dilakukan.

Secara keseluruhan, kombinasi antara steganografi menggunakan metode LSB dan enkripsi sederhana mampu menghasilkan sistem penyembunyian pesan dengan tingkat keamanan dasar yang fungsional dan mudah digunakan. Sistem ini sesuai digunakan sebagai solusi penyembunyian informasi pada citra digital serta sebagai media pembelajaran implementasi steganografi dan kriptografi sederhana.

REFERENSI

Aribowo, E., Amalya, W. S., & Puji Astuti, N. R. D. (2025). Application of LSB Steganography for Encrypted Data Using Triple Transposition Vigenere on Digital Images. *JUITA: Jurnal Informatika*, *13*(2), 157–165. https://doi.org/10.30595/juita.v13i2.24592

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.

Krisna, I Gusti Ngurah Febri Ananda Karyawati, A. E. (2024). *Penerapan Teknik Steganografi LSB pada Format Gambar Modern*. *2*, 673–680.

Patil, H. V, & Sonaje, V. P. (2024). Crypto-Stego: A Hybrid Method for Encrypting Text Messages or Text Files within Images Using AES and LSB Algorithms. *Original Research Paper International Journal of Intelligent Systems and*

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

JIKUM
JURNAL ILMU KOMPUTER

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

Applications in Engineering IJISAE, *2024*(23s), 2780–2793. www.ijisae.org

Rahman, S., Uddin, J., Hussain, H., Ahmed, A., Khan, A. A., Zakarya, M., Rahman, A., & Haleem, M. (2023). A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. *Scientific Reports*, *13*(1), 1–19. https://doi.org/10.1038/s41598-023-41303-1

S, A. M. R., & Hasanuddin, T. (2021). *Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography*. *2*(2), 91–102.

Putra, R. A., & Hidayat, R. (2022). Analisis metode Least Significant Bit (LSB) pada steganografi citra digital. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 9(4), 789–796.

Prasetyo, E., & Nugroho, A. (2022). Penerapan kriptografi klasik dalam pengamanan data digital. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 6(5), 873–880.

Siregar, R. R., & Ramadhan, A. (2023). Implementasi steganografi citra digital berbasis web menggunakan JavaScript. *Jurnal Informatika dan Rekayasa Perangkat Lunak*, 5(3), 211–219.

Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, O. D., & Wijanarto. (2022). *Teori pengolahan citra digital*. Yogyakarta: Andi.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.