**Jurnal Publikasi Manajemen Informatika**
**Volume 5 Nomor 2 Mei 2026**
E-ISSN : 2808-9014; P-ISSN 2808-9359, Hal 104-119
DOI: https://doi.org/10.55606/jupumi.v5i2.6743
*Tersedia*: https://journalcenter.org/index.php/jupumi

# PENERAPAN STEGANOGRAFI LSB DAN KRIPTOGRAFI AES-256 DALAM KEAMANAN FILE GAMBAR

**Suhada S. Yunus[1*], Yohanes Suban Belutowe[2], Benyamin Jago Belalawe[3]**

1,2,3 STIKOM UYELINDO Kupang, Indonesia
**suhadayunus4@gmail.com*, *yosube@gmail.com* dan *belalawe1308@gmail.com*

Alamat: Jl. Perintis Kemerdekaan 1 Kupang, Indonesia
*Korespondensi penulis: suhadayunus4@gmail.com*

***Abstract***. *Digital data security has become a crucial aspect in an era where information exchange is increasingly open, especially within government institutions that handle sensitive internal documents and messages. In the context of the Military Court III-15 Kupang, a security mechanism is required to ensure the confidentiality and integrity of messages during internal data transmission. This study applies a combination of the Least Significant Bit (LSB) steganography method and the Advanced Encryption Standard 256-bit (AES-256) cryptographic algorithm to enhance the security of text messages. The text message is first encrypted using AES-256 to generate ciphertext, which is then embedded into a Portable Network Graphics (PNG) image by manipulating the least significant bits of its pixels using the LSB method. The result of this research is a web-based application implementing LSB steganography and AES-256 cryptography for securing image files, specifically designed to support the internal information security needs of the Military Court III-15 Kupang. The combination of both methods provides a dual-layer security mechanism, ensuring that the hidden message remains protected even if the image file is transferred or accessed by unauthorized parties.*

***Keywords***: *AES-256, Cryptography, Data Security, LSB, Steganography.*

**Abstrak**. Keamanan data digital menjadi aspek penting di era pertukaran informasi yang semakin terbuka, terutama pada instansi pemerintah yang menangani dokumen dan pesan internal bersifat sensitif. Dalam konteks Pengadilan Militer III-15 Kupang, diperlukan sebuah mekanisme pengamanan informasi yang mampu menjaga kerahasiaan serta integritas pesan selama proses pertukaran data internal. Penelitian ini menerapkan kombinasi metode steganografi *Least Significant Bit* (LSB) dan algoritma kriptografi *Advanced Encryption Standard* 256-bit (AES-256) untuk meningkatkan keamanan pesan teks. Pesan teks terlebih dahulu dienkripsi menggunakan AES-256 sehingga menghasilkan *ciphertext*, kemudian disisipkan ke dalam citra digital berformat *Portable Network Graphics* (PNG) dengan memanipulasi bit paling rendah pada piksel menggunakan metode LSB. Hasil penelitian berupa aplikasi berbasis website steganografi LSB dan kriptografi AES-256 dalam keamanan file gambar yang diimplementasikan khusus untuk mendukung kebutuhan keamanan pertukaran informasi internal di Pengadilan Militer III-15 Kupang. Kombinasi kedua metode tersebut memberikan lapisan perlindungan ganda, sehingga pesan tetap aman meskipun file gambar berpindah tangan atau diakses oleh pihak yang tidak berwenang.

**Kata kunci**: AES-256, Kriptografi, Keamanan Data, LSB, Steganografi.

## 1. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi saat ini telah membawa perubahan besar dalam cara manusia menyimpan, mengolah, dan mengirimkan data. Setiap hari, miliaran informasi digital dipertukarkan melalui internet, mulai dari pesan pribadi, dokumen rahasia, hingga informasi penting pada lembaga pemerintahan. Kondisi ini membuat kebutuhan terhadap sistem keamanan informasi semakin mendesak, terutama pada instansi yang menangani data sensitif seperti Pengadilan Militer III-15

*Naskah Masuk: 12 Januari 2026; Revisi: 12 Februari 2026; Diterima: 12 Maret 2026; Tersedia: 12 April 2026; Terbit: 17 Mei 2026;*

Kupang, yang dalam aktivitas internalnya sering melakukan pertukaran informasi terkait proses penyidikan, administrasi perkara, dan komunikasi antarbagian yang bersifat rahasia. Tanpa mekanisme pengamanan yang memadai, informasi tersebut berpotensi mengalami penyadapan, kebocoran, atau akses oleh pihak yang tidak berwenang. Situasi ini sejalan dengan temuan (Ladzuardy, et.al., 2024), yang menyatakan bahwa meningkatnya penggunaan layanan digital di berbagai sektor di Indonesia menuntut ketersediaan sistem keamanan data yang kuat dan sulit ditembus.

Salah satu teknik yang banyak diteliti untuk melindungi data adalah steganografi, yaitu teknik menyembunyikan pesan ke dalam media digital sehingga keberadaan pesan tersebut tidak disadari oleh pihak luar. Metode yang paling populer adalah *Least Significant Bit* (LSB) karena mampu menyisipkan informasi tanpa menyebabkan perubahan visual yang mencolok. Menurut Muh. Akbar dan Alam (2025), kombinasi metode *Least Significant Bit* (LSB) dengan enkripsi *Advanced Encryption Standard 256-bit* (AES-256) dapat menyembunyikan pesan dengan aman ke dalam citra digital dengan kualitas gambar tetap tinggi, ditunjukkan melalui nilai *Peak Signal to Noise Ratio* (PSNR) yang tetap stabil setelah proses penyisipan. Penggunaan format *Portable Network Graphics* (PNG), yang bersifat lossless, juga mendukung keberhasilan metode ini karena menjaga integritas bit-bit piksel saat proses penyisipan dilakukan.

Penelitian terkini memperkuat temuan tersebut. Ibnu, et.al (2023) menunjukkan bahwa integrasi steganografi dan kriptografi mampu menghasilkan citra stego yang sulit dibedakan dari citra aslinya, sekaligus menjaga kerahasiaan pesan yang disisipkan. Artinya, pendekatan ganda ini tidak hanya menyembunyikan data, tetapi juga melindunginya secara kriptografis apabila pesan berhasil diekstraksi oleh pihak yang tidak berkepentingan.

Di sektor kesehatan, Hernandi dan Chandra (2024) juga membuktikan bahwa *Advanced Encryption Standard 256-bit* (AES-256) mampu melindungi data sensitif seperti rekam medis dari ancaman kebocoran data, sehingga semakin menguatkan posisi *Advanced Encryption Standard 256-bit* (AES-256) sebagai algoritma kriptografi modern yang kuat.

Beberapa penelitian Indonesia telah menerapkan kombinasi steganografi dan kriptografi, namun sebagian masih menggunakan algoritma klasik seperti *Vigenere Cipher* atau *Triple Data Encryption Standard* (*Triple* DES). Septa, et.al (2020) menggunakan *Vigenere Cipher* sebelum proses penyisipan, tetapi metode ini lemah

karena mudah dipecahkan. Sementara Adityan, et.al (2023) menggunakan Triple DES yang lebih kuat, namun tetap memiliki kelemahan dalam keamasnan dan performa jika dibandingkan dengan *Advanced Encryption Standard 256-bit* (AES-256). Dengan demikian, penggunaan AES-256 sebagai pengganti algoritma terdahulu sangat relevan untuk meningkatkan keamanan pesan secara signifikan.

Dari berbagai penelitian tersebut dapat disimpulkan bahwa integrasi antara steganografi *Least Significant Bit* **(**LSB) dan kriptografi *Advanced Encryption Standard 256-bit* (AES-256) merupakan salah satu pendekatan paling aman dan efektif untuk menjaga kerahasiaan data digital. Pesan yang disembunyikan tidak hanya tersembunyi dalam media digital, tetapi juga dilindungi oleh enkripsi modern sehingga tetap aman meskipun berhasil diekstraksi secara ilegal. Pendekatan hybrid ini tidak hanya meningkatkan keamanan tetapi juga memberikan lapisan proteksi ganda terhadap ancaman pencurian maupun penyalahgunaan data.

Melalui penelitian ini diharapkan dapat dihasilkan sebuah sistem keamanan berbasis *website* yang kuat, mudah digunakan, dan mampu menjawab tantangan keamanan informasi di era digital. Selain itu, penelitian ini diharapkan memberikan solusi praktis untuk meningkatkan keamanan pertukaran informasi di lingkungan Pengadilan Militer III-15 Kupang, serta memperkaya literatur terkait integrasi steganografi *Least Significant Bit* (LSB) dan kriptografi *Advanced Encryption Standard 256-bit* (AES-256) yang masih jarang dieksplorasi secara mendalam di Indonesia.

## 2. KAJIAN TEORITIS

Beberapa penelitian terdahulu menunjukkan bahwa kombinasi steganografi dan kriptografi merupakan pendekatan yang efektif dalam meningkatkan keamanan pesan digital. Penerapan steganografi citra digital menggunakan metode Least Significant Bit (LSB) yang dikombinasikan dengan enkripsi Advanced Encryption Standard 256-bit (AES-256) mampu menyisipkan pesan secara aman tanpa menurunkan kualitas visual citra secara signifikan, serta memberikan perlindungan tambahan melalui enkripsi modern (Muh. Akbar dan Alam, 2025).

Pengembangan aplikasi berbasis *website* dengan integrasi metode steganografi dan modifikasi kriptografi *Advanced Encryption Standard* (AES) pada bagian *SubBytes*.

Sistem berbasis *website* yang dikembangkan memungkinkan pengguna untuk menyisipkan dan mengekstrak pesan rahasia dengan lebih mudah, sambil tetap menjamin keamanan data berkat enkripsi *Advanced Encryption Standard* (AES) yang dimodifikasi (Muh. Ilham, et.al 2024). Hasil penelitian menunjukkan bahwa platform berbasis *website* dapat meningkatkan efektivitas dan efisiensi penggunaan metode keamanan ini.

Penelitian selanjutnya menerapkan *Least Significant Bit* (LSB) pada file bitmap 24-bit yang dipadukan dengan enkripsi *Advanced Encryption Standard* (AES). Pesan teks dienkripsi terlebih dahulu menggunakan *Advanced Encryption Standard* (AES), kemudian disisipkan ke dalam dua bit terakhir dari setiap komponen warna piksel gambar. Hasil pengujian menunjukkan kapasitas penyisipan pesan cukup tinggi, kualitas visual tetap terjaga, dan perubahan visual tidak mudah terdeteksi secara kasat mata. Penelitian ini membuktikan bahwa kombinasi *Least Significant Bit* (LSB) dan *Advanced Encryption Standard* (AES) dapat menyembunyikan pesan secara efektif tanpa mengurangi kualitas citra (Marwa dan Wulan, 2023)

## 3. METODE PENELITIAN

### Bahan dan Alat Penelitian

Bahan yang digunakan dalam penelitian ini meliputi file gambar berformat PNG yang berfungsi sebagai media penampung (cover image) serta teks pesan rahasia yang akan disisipkan ke dalam gambar. Format PNG dipilih karena mampu mempertahankan kualitas citra dengan baik dan mendukung proses penyisipan pesan tanpa mengurangi kualitas gambar.

Tabel 1. Data Gambar

| No | Gambar 1 | Gambar 2 | Gambar 3 |
|---|---|---|---|
| 1 |  |  |  |

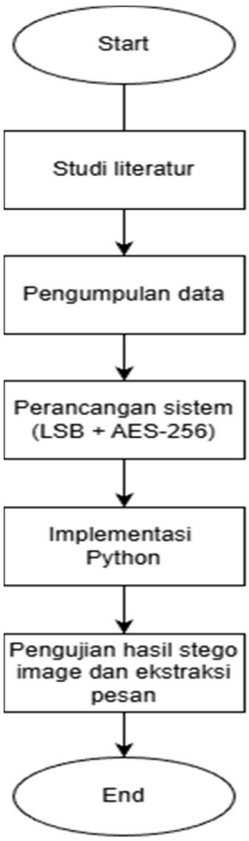
| | | | |
|---|---|---|---|
| 2 |  |  |  |

Pada penelitian ini, penulis memanfaatkan alat penelitian yang terdiri dari hardware dan software sebagai pendukung dalam proses pengerjaannya. Adapun peralatan yang digunakan antara lain: :

1. Perangkat Keras (*Hardware*)
    1. Laptop DESKTOP-1I5H3RH
    2. Processor MD Ryzen 3 5300U with Radeon Graphics (2.60 GHz)
    3. Kapasitas RAM 12 GB
    4. Penyimpanan internal SSD 512 GB
2. Perangkat Lunak (*Software*)
    1. Windows 11 Pro
    2. Microsoft 2019
    3. Mendeley-Desktop
    4. Visual Studio Code
    5. Python 3.12
    6. Library Pendukung : Flask, Pillow, Cryptography dan Numpy
    7. Google Chrome
    8. ExifTool

**Prosedur Penelitian**

Dalam tahap penelitian ini terdapat proses atau tahapan yang dilakukan oleh penulis dalam perancangan aplikasi berbasi *website* yang akan dibangun dengan melakukan studi literatur hingga selesai. Berikut *flowchart* prosedur penelitian:

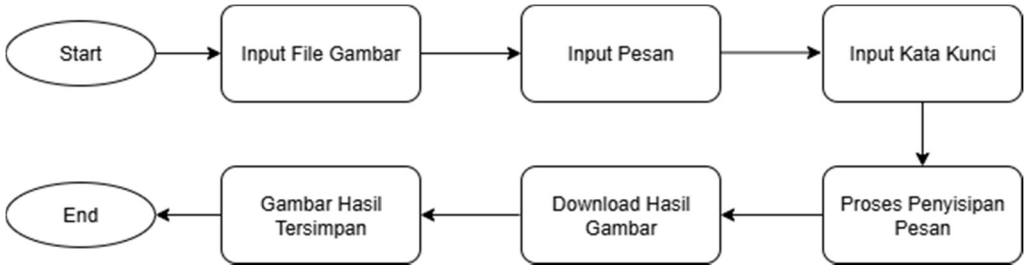



**Gambar 1. *Flowchart* Penelitian**

Flowchart pada gambar 1 menunjukkan tahapan penelitian yang dilakukan secara sistematis. Penelitian diawali dengan tahap studi literatur, yaitu mempelajari teori dan penelitian terdahulu yang berkaitan dengan steganografi *Least Significant Bit* (LSB) dan kriptografi *Advanced Encryption Standard 256-bit* (AES-256) sebagai dasar pengembangan sistem. Selanjutnya dilakukan pengumpulan data, berupa pemilihan file gambar berformat PNG sebagai media penampung serta penyiapan teks pesan rahasia yang akan disisipkan.

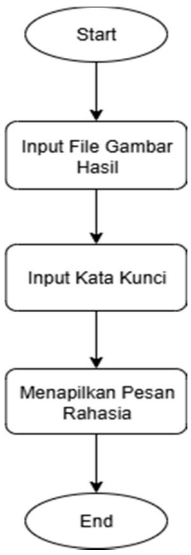
Tahap berikutnya adalah perancangan sistem, yang meliputi perancangan alur proses enkripsi pesan menggunakan AES-256 dan penyisipan pesan terenkripsi ke dalam gambar menggunakan metode LSB. Setelah perancangan selesai, sistem diimplementasikan menggunakan bahasa pemrograman *Python* sesuai dengan desain yang telah dibuat. Tahap akhir penelitian adalah pengujian hasil *stego image* dan proses ekstraksi pesan, untuk memastikan pesan dapat disisipkan dan diekstraksi kembali dengan benar serta kualitas visual gambar tetap terjaga.

**Tahapan Penyisipan dan Ekstraksi Pesan**




**Gambar 2. *Diagram* Alur Proses Penyisipan Pesan**

*Diagram* alur penyisipan pesan diawali dengan proses input file gambar oleh pengguna yang berfungsi sebagai media penampung pesan. Setelah gambar dipilih, pengguna memasukkan pesan rahasia yang akan disisipkan serta kata kunci sebagai kunci enkripsi. Sistem kemudian menjalankan proses penyisipan pesan dengan terlebih dahulu mengenkripsi pesan menggunakan algoritma *Advanced Encryption Standard 256-bit* (AES-256), lalu menyisipkan hasil enkripsi tersebut ke dalam gambar menggunakan metode *Least Significant Bit* (LSB). Setelah proses penyisipan selesai, sistem menghasilkan stego image yang dapat diunduh oleh pengguna dan disimpan sebagai gambar hasil penyisipan pesan.




**Gambar 3. *Diagram* Alur Proses Ekstrak Pesan**

Tahapan ekstraksi pesan dimulai dengan pengguna mengunggah file gambar hasil penyisipan (*stego image*) ke dalam sistem. Selanjutnya, pengguna memasukkan kata kunci yang sama dengan kunci yang digunakan pada saat proses penyisipan pesan. Sistem kemudian mengekstraksi data pesan dari bit paling tidak signifikan pada piksel gambar

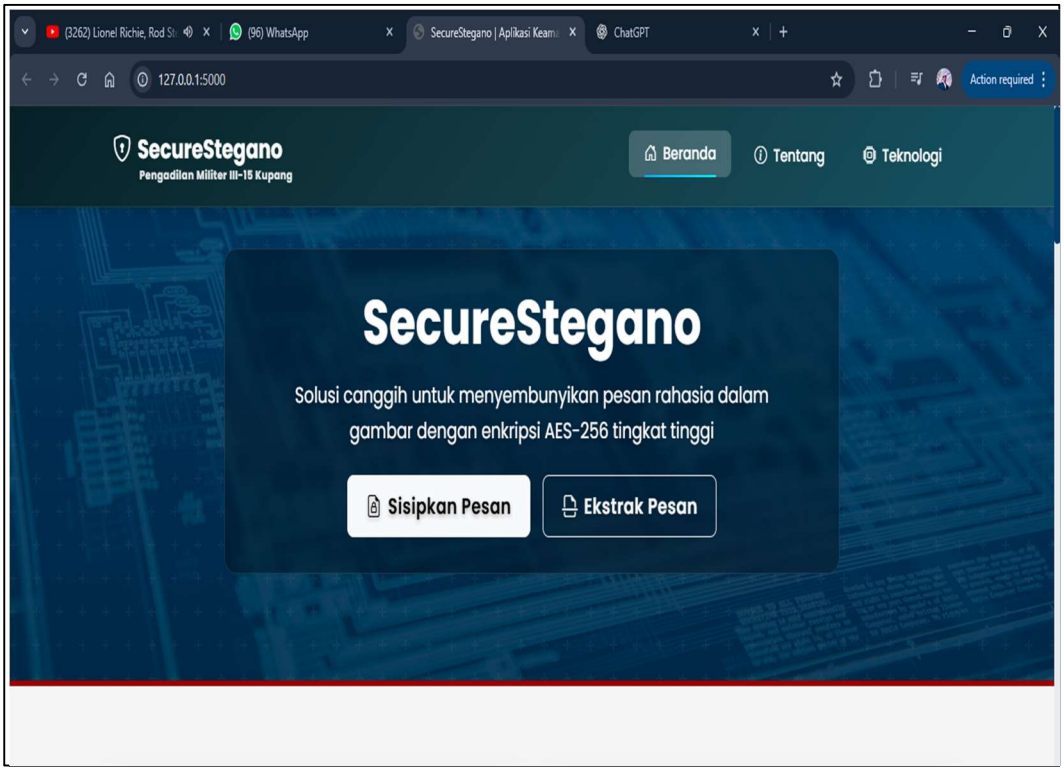
menggunakan metode *Least Significant Bit* (LSB) dan melakukan proses dekripsi menggunakan algoritma *Advanced Encryption Standard 256-bit* (AES-256). Apabila kata kunci yang dimasukkan sesuai, sistem akan berhasil menampilkan kembali pesan rahasia dalam bentuk teks asli (*plaintext*) kepada pengguna.

## 4. HASIL DAN PEMBAHASAN

### Implementasi Sistem

1. Halaman Utama

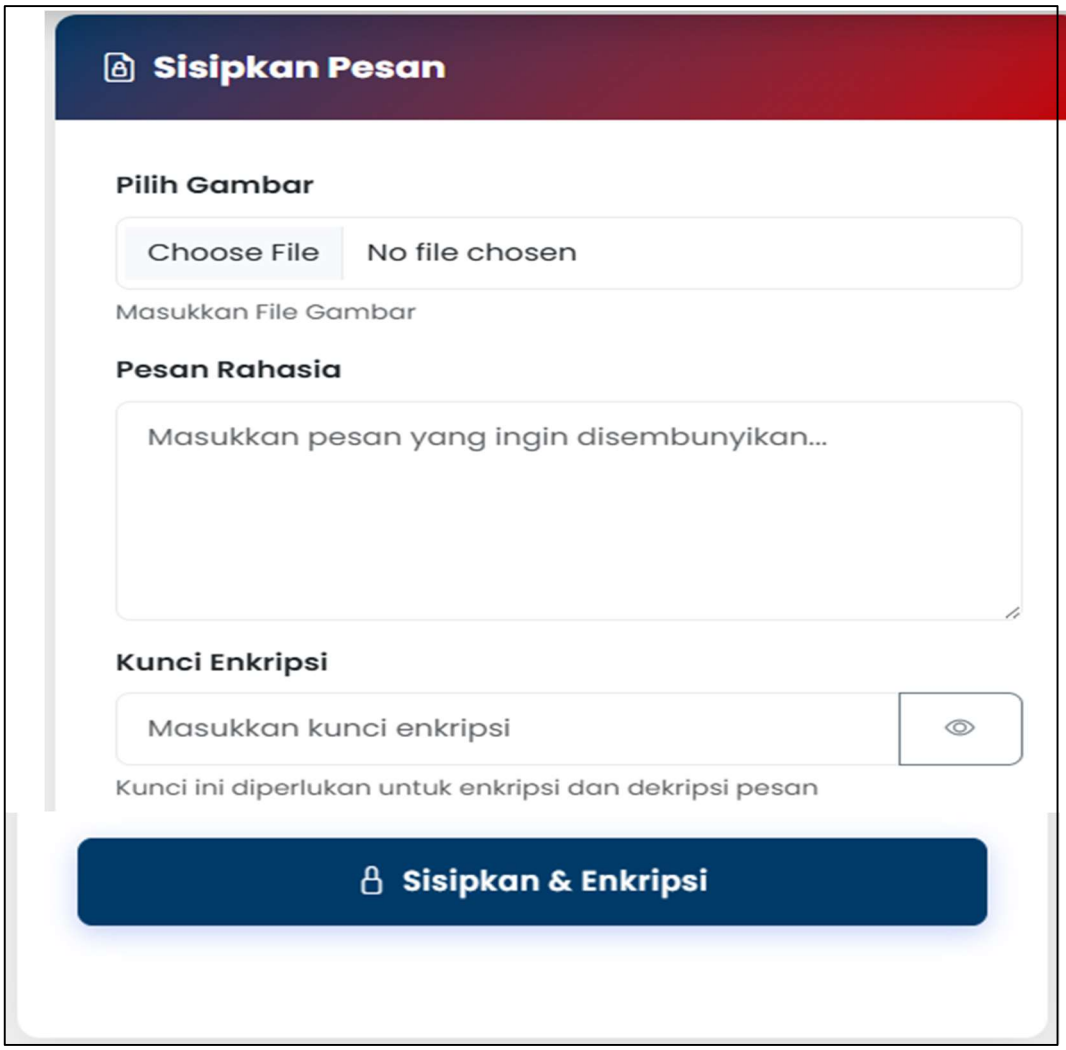
   Halaman utama merupakan tampilan awal sistem yang berfungsi sebagai pusat interaksi pengguna. Pada halaman ini disediakan dua fitur utama, yaitu sisipkan pesan dan ekstrak pesan, yang memungkinkan pengguna untuk menyembunyikan pesan ke dalam media gambar serta mengambil kembali pesan yang telah disisipkan secara mudah dan terstruktur.




**Gambar 4. Halaman Utama**

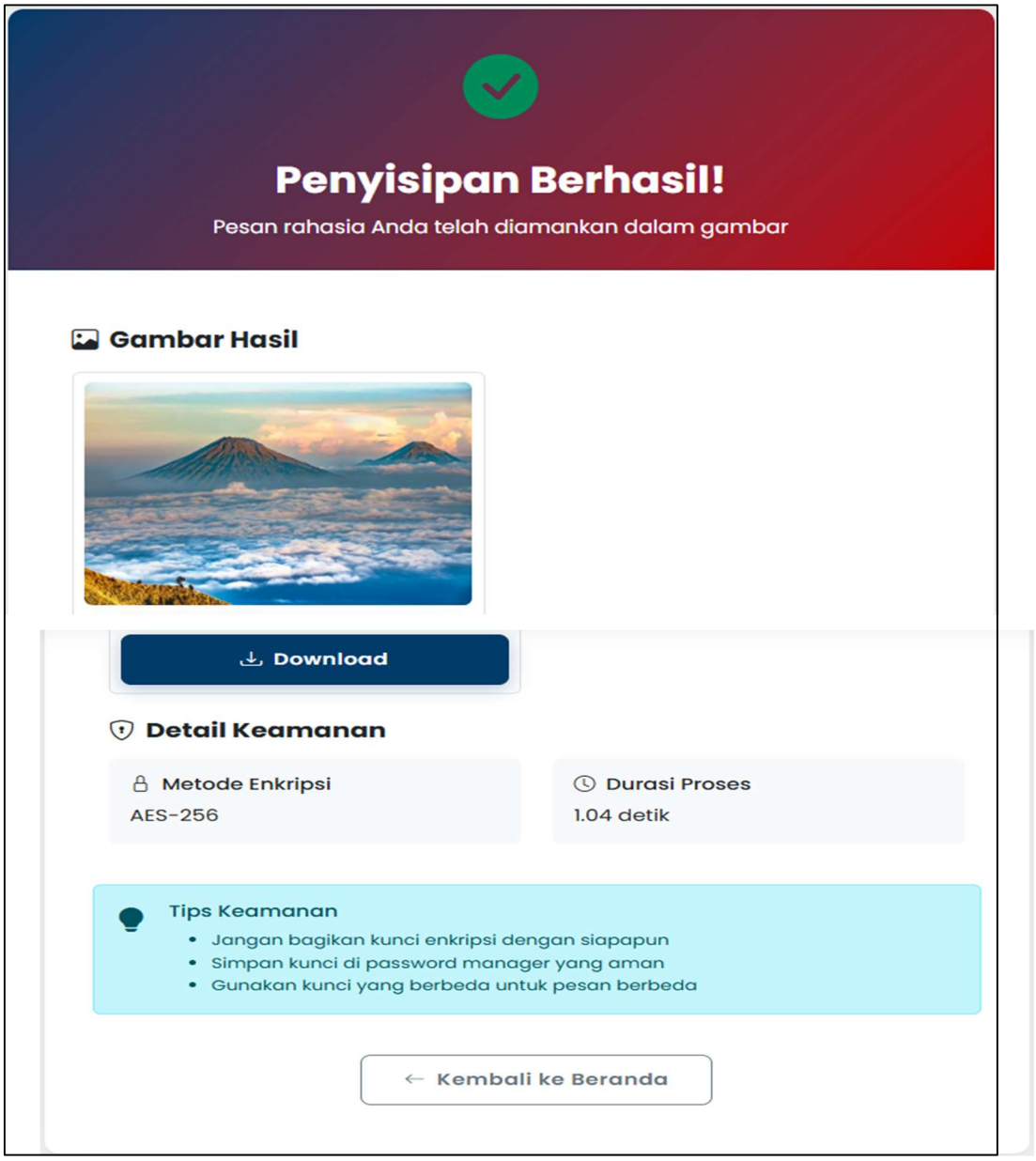
2. Halaman Penyisipan Pesan

   Halaman penyisipan pesan merupakan halaman yang digunakan untuk melakukan proses penyisipan pesan rahasia ke dalam media gambar. Pada halaman ini, pengguna terlebih dahulu melakukan proses input gambar yang akan digunakan sebagai media penyimpanan, kemudian memasukkan pesan rahasia yang akan disisipkan serta kunci enkripsi sebagai pengaman pesan. Setelah seluruh data dimasukkan, sistem akan melakukan proses steganografi dengan mengombinasikan metode *Least Significant Bit* (LSB) dan algoritma enkripsi *Advanced Encryption Standard 256-bit* (AES-256) untuk menghasilkan gambar hasil penyisipan (*stegano image*)




**Gambar 5. Halaman Penyisipan Pesan**

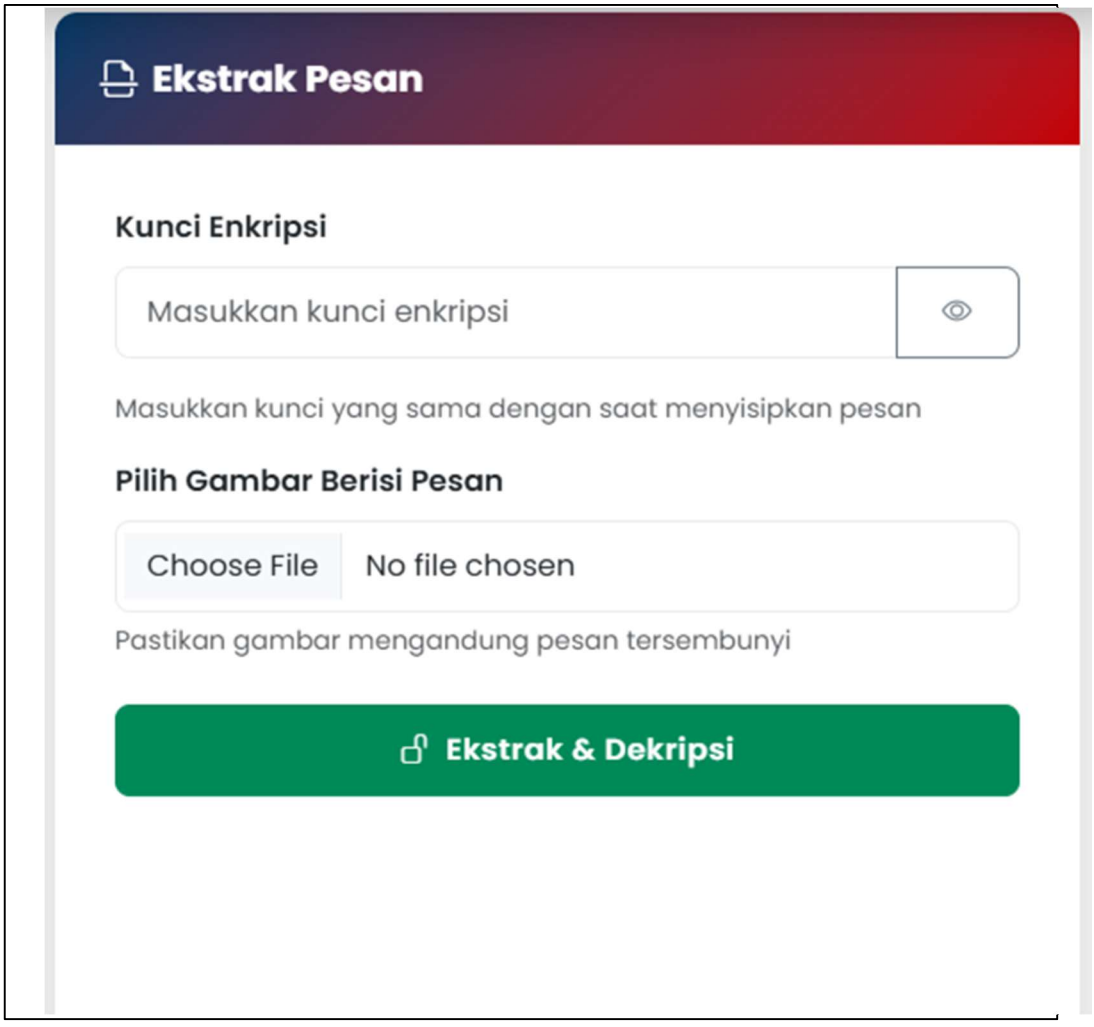
Setelah pengguna melakukan proses penyisipan sistem akan menghasilkan gambar stego image yang berisi pesan yang rahasia yang telah di sisipkan. Pada halaman ini, pengguna dapat melihat stego image sebagai hasil akhir dari proses penyisipan. Selain itu, sistem menyediakan fitur untuk mengunduh gambar tersebut agar dapat disimpan atau digunakan kembali. Gambar hasil penyisipan selanjutnya dapat digunakan pada proses ekstraksi melalui form ekstrak pesan, sehingga pesan rahasia yang tersembunyi di dalam gambar dapat didekripsi dan ditampilkan kembali oleh sistem.




**Gambar 6. Halaman Setelah Penyisipan Pesan**

3. Halaman Ekstraksi Pesan

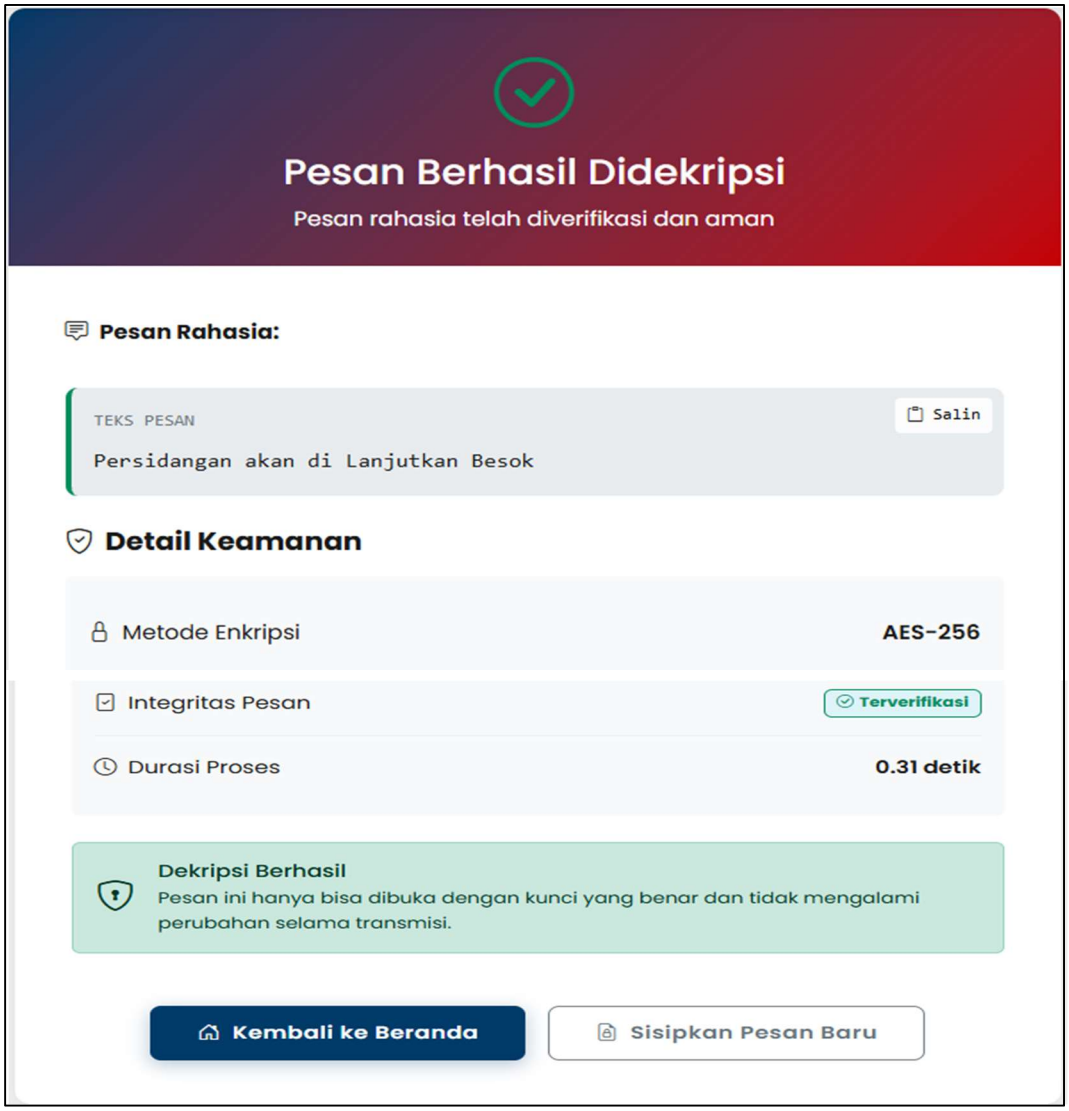
Halaman Ekstraksi Pesan merupakan halaman yang digunakan untuk melakukan proses pengambilan kembali pesan rahasia yang telah disisipkan ke dalam media gambar. Pada halaman ini, pengguna melakukan proses input gambar hasil penyisipan serta memasukkan kunci enkripsi yang sesuai. Selanjutnya, sistem akan melakukan proses ekstraksi pesan menggunakan metode *Least Significant Bit* (LSB) dan mendekripsi pesan menggunakan algoritma *Advanced Encryption Standard 256-bit* (AES-256), sehingga pesan rahasia dapat ditampilkan kembali dalam bentuk teks asli (*plaintext*).




**Gambar 7. Halaman Ekstrksi Pesan**

Setelah gambar hasil penyisipan disimpan, pengguna dapat mengirimkan gambar tersebut kepada pihak tujuan dengan menggunakan dokumen pada aplikasi *WhatsApp*, selanjutnya pengguna dapat melakukan proses ekstraksi di fitur ekstrak pesan untuk mengetahui isi pesan didalamnya. Setelah melakukan

proses tersebut pengguna dapat melihat isi pesan rahasia secara jelas dan aman sesuai dengan kunci enkripsi yang digunakan.




**Gambar 8. Halaman Dekripsi Pesan**

**Pengujian Sistem**

Pengujian sistem dilakukan untuk memastikan bahwa aplikasi steganografi berbasis website yang mengintegrasikan metode *Least Significant Bit* (LSB) dan algoritma kriptografi *Advanced Encryption Standard 256-bit* (AES-256) berjalan sesuai dengan tujuan dan kebutuhan yang telah ditetapkan. Pengujian ini difokuskan pada pengujian fungsionalitas sistem, keakuratan proses enkripsi dan dekripsi, serta keberhasilan proses penyisipan dan ekstraksi pesan rahasia pada file gambar.

### *Black Box Testing*

Pengujian sistem pada penelitian ini menggunakan metode *Black Box Testing*, yaitu pengujian fungsional yang menilai kinerja sistem berdasarkan masukan dan keluaran tanpa memperhatikan struktur kode program. Pengujian dilakukan pada proses penyisipan dan ekstraksi pesan untuk memastikan sistem mampu mengenkripsi pesan menggunakan *Advanced Encryption Standard 256-bit* (AES-256), menyisipkannya ke dalam gambar dengan metode *Least Significant Bit* (LSB), serta mengekstrak dan mendekripsi kembali pesan dengan benar sesuai tujuan penelitian.

Tabel 2. Pengujian Fitur Penyisipan Pesan

| No | Fitur | Input | Output yang Diharapkan | Hasil |
|---|---|---|---|---|
| 1 | Upload gambar | File PNG | Gambar diterima sistem | Berhasil |
| 2 | Input pesan dan kunci | Teks dan kata kunci | Data diproses sistem | Berhasil |
| 3 | Enkripsi dan embedding | Pesan dan gambar | Stego image terbentuk | Berhasil |
| 4 | Unduh hasil | Stego image | File dapat diunduh | Berhasil |

Tabel 3. Pengujian Fitur Ekstraksi Pesan

| No | Fitur | Input | Output yang Diharapkan | Hasil |
|---|---|---|---|---|
| 1 | Upload stego image | File PNG | Gambar diterima sistem | Berhasil |
| 2 | Input kunci | Kata kunci benar | Data diproses sistem | Berhasil |
| 3 | Ekstraksi dan dekripsi | Stego image | Pesan asli ditampilkan | Berhasil |

**Pengujian Penyisipan dan Ekstraksi Pesan**

Hasil pengujian pada tabel 4 dan 5 menunjukkan bahwa sistem berhasil melakukan proses penyisipan dan ekstraksi pesan rahasia pada file gambar berformat PNG menggunakan kombinasi metode *Least Significant Bit* (LSB) dan algoritma kriptografi *Advanced Encryption Standard 256-bit* (AES-256). Setiap pesan yang dienkripsi dan disisipkan ke dalam gambar (*stego image*) dapat diekstraksi kembali dengan baik dan menghasilkan pesan asli (*plaintext*) yang identik dengan pesan awal, dengan syarat kunci enkripsi yang digunakan pada proses ekstraksi sama dengan kunci yang digunakan pada saat penyisipan pesan. Selain itu, hasil pengujian juga menunjukkan bahwa proses penyisipan dan ekstraksi pesan dapat dilakukan tanpa menimbulkan perubahan visual yang signifikan pada gambar, serta stego image yang dihasilkan dapat diunduh dan digunakan kembali oleh pengguna. Durasi proses penyisipan dan ekstraksi pesan juga dipengaruhi oleh panjang pesan yang diproses, di mana semakin banyak karakter pesan yang disisipkan, maka waktu pemrosesan yang dibutuhkan sistem akan semakin meningkat.

Tabel 4. Hasil Pengujian

| No | Cover Image | Pesan | Kunci | Hasil |
|---|---|---|---|---|
| 1 |  | Terdakwa Imam di Bebaskan Karena Tidak Bersalah | Terdakwa1 |  |
| 2 |  | Terdakwa Nugraha di Hukum Mati | Terdakwa2 |  |
| 3 |  | Terdakwa Imron di Penjara 5 Tahun | Terdakwa3 |  |
| 4 |  | Persidangan Luki Berlangsung Selama 1 Bulan | Persidangan1 |  |
| 5 |  | Persidangan akan di Lanjutkan Besok | Persidangan2 |  |
| 6 |  | Persidangan Bersifat Tertutup Harap di Rahasikan Sidang Ini | Persidangan3 |  |

Tabel 5. Hasil Pengujian Status dan Durasi

| No | Status Embedd | Status Extract | Durasi Embedd | Durasi Extract |
|---|---|---|---|---|
| 1 | Berhasil | Berhasil | 0.20 Detik | 0.14 Detik |
| 2 | Berhasil | Berhasil | 2.45 Detik | 0.41 Detik |
| 3 | Berhasil | Berhasil | 0.17 Detik | 0.15 Detik |
| 4 | Berhasil | Berhasil | 0.68 Detik | 0.19 Detik |
| 5 | Berhasil | Berhasil | 0.49 Detik | 0.18 Detik |
| 6 | Berhasil | Berhasil | 0.28 Detik | 0.17 Detik |

## 5. KESIMPULAN DAN SARAN

### Kesimpulan

Berdasarkan hasil penelitian mengenai penerapan steganografi LSB dan kriptografi AES-256 dalam keamanan file gambar, dapat disimpulkan bahwa proses penyisipan pesan rahasia berhasil dilakukan dengan baik, di mana pesan teks terenkripsi dapat disisipkan dan diekstraksi kembali secara utuh menggunakan kunci enkripsi yang sama. Dari sisi performa, proses penyisipan dan ekstraksi pesan berlangsung cepat dan efisien, durasi penyisipan berkisar antara 0,14–2,45 detik, sedangkan ekstraksi 0,15–0,41 detik, dengan waktu pemrosesan dipengaruhi oleh panjang pesan, namun secara umum berada di bawah 3 detik untuk gambar berukuran kecil hingga menengah, sehingga sistem layak digunakan untuk pengamanan pesan berbasis citra digital.

### Saran

1. Untuk mengurangi noise dan menjaga kualitas visual gambar, disarankan menggunakan gambar beresolusi tinggi serta membatasi jumlah pesan yang disisipkan, dengan pengembangan teknik LSB adaptif agar perubahan piksel lebih terkendali.
2. Kecepatan proses penyisipan dan ekstraksi pesan dapat ditingkatkan melalui optimasi algoritma enkripsi dan pengolahan citra digital. Untuk menjaga keseimbangan antara performa dan kualitas gambar, jumlah karakter pesan sebaiknya dibatasi sesuai kapasitas gambar, misalnya tidak melebihi 30–40% dari kapasitas piksel, serta dilengkapi fitur perhitungan otomatis jumlah karakter maksimum berdasarkan resolusi gambar.

## DAFTAR REFERENSI

Festi, S., Jaya, B., Kuway, S. M., & Syarifudin, G. (2020). Perancangan Perangkat Lunak Steganografi Menggunakan Least Significant Bit Dengan Enkripsi Vigenere Cipher. *E-Jurnal JUSITI (Jurnal Sistem Informasi Dan Teknologi Informasi)*, *9*(1), 52–64. https://ejurnal.undipa.ac.id/index.php/jusiti/article/view/643/559

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://journal.eng.unila.ac.id/index.php/jitet/article/view/5620/2268

Halim, M., & Wulan Sri Lestari. (2023). Steganography Menggunakan Advanced Encryption Standard dan Metode Least Significant Bit pada File Bitmap 24-bit. *Jurnal Armada Informatika*, *7*(2), 295–300. https://jurnal.stmikmethodistbinjai.ac.id/jai/article/view/76/74

Islami, L., Akbar, H. P., & Rizal, R. G. (2024). *Sistem Keamanan Informasi Di Era Digital*. *1*(11),1174–1177. https://jurnalmahasiswa.com/index.php/jriin/article/view/1150/735

Kurniawan, M. I., Maryanto, E., & Rahayu, S. P. (2024). Implementation of a Combination of Advanced Encryption Standard Cryptography With Subbytes Modification and Steganography Based on a Website. *Jurnal Teknik Informatika (Jutif)*, *5*(5), 1375–1384. https://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/2665/654

Mulyono, I. U. W., Kusumawati, Y., & Ningrum, N. K. (2023). Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher. *Jurnal Masyarakat Informatika*, *14*(1), 16–28. https://ejournal.undip.ac.id/index.php/jmasif/article/view/51484/23965

R.M. Hilmy Hernandi, & Joko Christian Chandra. (2024). Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya. *KRESNA: Jurnal Riset Dan Pengabdian Masyarakat*, *4*(1), 12–22. https://jurnaldrpm.budiluhur.ac.id/index.php/Kresna/article/view/131/138

Wisnu, A., Prasetya, Y., Suhardjo, B., & Munir, R. (2023). Penggunaan Kombinasi Kriptografi Triple DES dan Teknik Steganografi LSB dalam Mengamankan Pesan Militer. *Jurnal SISTEM INFORMASI Dan TEKNOLOGI INFORMASI*, *12*(2), 193–199. https://ejurnal.undipa.ac.id/index.php/jusiti/article/view/1431/1066