Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

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

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

[1,2,3] Program Studi Teknik Informatika, STIKOM Uyelindo Kupang
Jl Perwira no III Kupang, Indonesia

suhadayunus4@gmail.com, yosube@gmail.com & belalawe1308@gmail.com

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.

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*.

1 Pendahuluan (or Introduction)

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

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 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, yang menyatakan bahwa meningkatnya penggunaan layanan digital di berbagai sektor di Indonesia menuntut ketersediaan sistem keamanan data yang kuat dan sulit ditembus [1].

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. 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 [2].

Penelitian terkini memperkuat temuan tersebut dengan menunjukkan bahwa integrasi steganografi dan kriptografi mampu menghasilkan citra stego yang sulit dibedakan dari citra aslinya, sekaligus menjaga kerahasiaan pesan yang disisipkan [3]. Artinya, pendekatan ganda ini tidak hanya menyembunyikan data, tetapi juga melindunginya secara kriptografis apabila pesan berhasil diekstraksi oleh pihak yang tidak berkepentingan.

Meskipun steganografi dapat menyembunyikan pesan dengan baik, teknik ini belum menjamin keamanan penuh, karena pesan yang disisipkan masih dapat diekstraksi jika metode penyisipannya diketahui. Oleh karena itu, penggunaan kriptografi tambahan seperti Advanced Encryption Standard 256-bit (AES-256) menjadi sangat penting. Penelitian juga menunjukkan bahwa AES-256 telah berhasil menjaga kerahasiaan dokumen rahasia di lingkungan pemerintahan, sehingga relevan digunakan dalam sistem keamanan tingkat tinggi [4].

Di sektor kesehatan 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 [5].

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). Ada yang menggunakan *Vigenere Cipher* sebelum proses penyisipan, tetapi metode ini lemah karena mudah dipecahkan [6]. Sementara ada juga yang menggunakan Triple DES yang lebih kuat, namun tetap memiliki kelemahan dalam keamanan dan performa jika dibandingkan dengan *Advanced Encryption Standard 256-bit* (AES-256) [7]. Dengan demikian, penggunaan AES-256 sebagai pengganti algoritma terdahulu sangat relevan untuk meningkatkan keamanan pesan secara signifikan.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

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 Tinjauan Literatur (or Literature Review)

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 [2].

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 [8]. 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 [9].

Berdasarkan beberapa penelitian tersebut, dapat disimpulkan bahwa integrasi steganografi *Least Significant Bit* (LSB) dengan kriptografi *Advanced Encryption Standard* (AES) merupakan pendekatan yang tepat untuk membangun sistem keamanan pesan digital yang aman, efisien, dan praktis untuk diterapkan.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

3 Metode Penelitian (or Research Method)

3.1 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: :

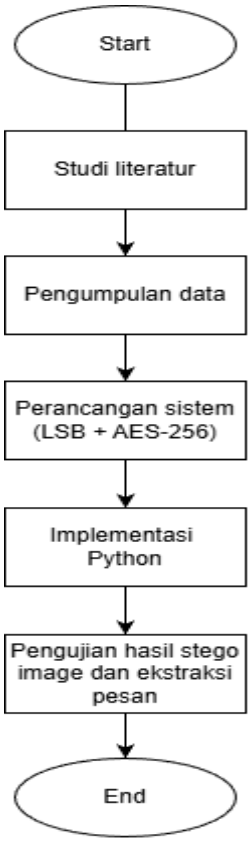
1. Perangkat Keras (*Hardware*)
    1. Laptop DESKTOP-1I5H3RH
    2. Processor MD Ryzen 3 5300U with Radeon Graphics (2.60 GHz)
    3. Kapasitas RAM 12 GB
    4. Penyimpanan internal SSD 512 GB
2. Perangkat Lunak (*Software*)
    1. Windows 11 Pro
    2. Microsoft 2019
    3. Mendeley-Desktop
    4.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

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

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

3.2 Tahapan Penelitian



Gambar 1. *Flowchart* Penelitian 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.

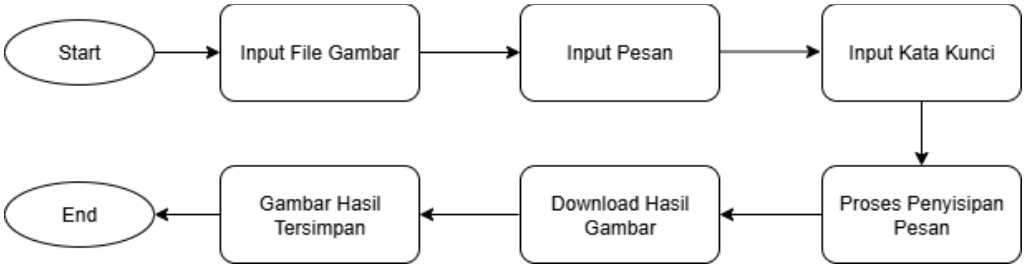
Tahap berikutnya adalah perancangan sistem, yang meliputi perancangan alur proses enkripsi pesan menggunakan AES-256 dan penyisipan pesan terenkripsi ke dalam gambar menggunakan metode LSB. Setelah perancangan selesai, sistem diimplementasikan menggunakan bahasa pemrograman *Python* sesuai dengan desain 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.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

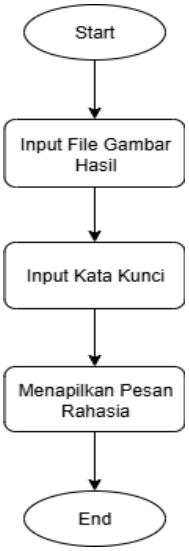
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

3.3 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 Ekstak

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.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

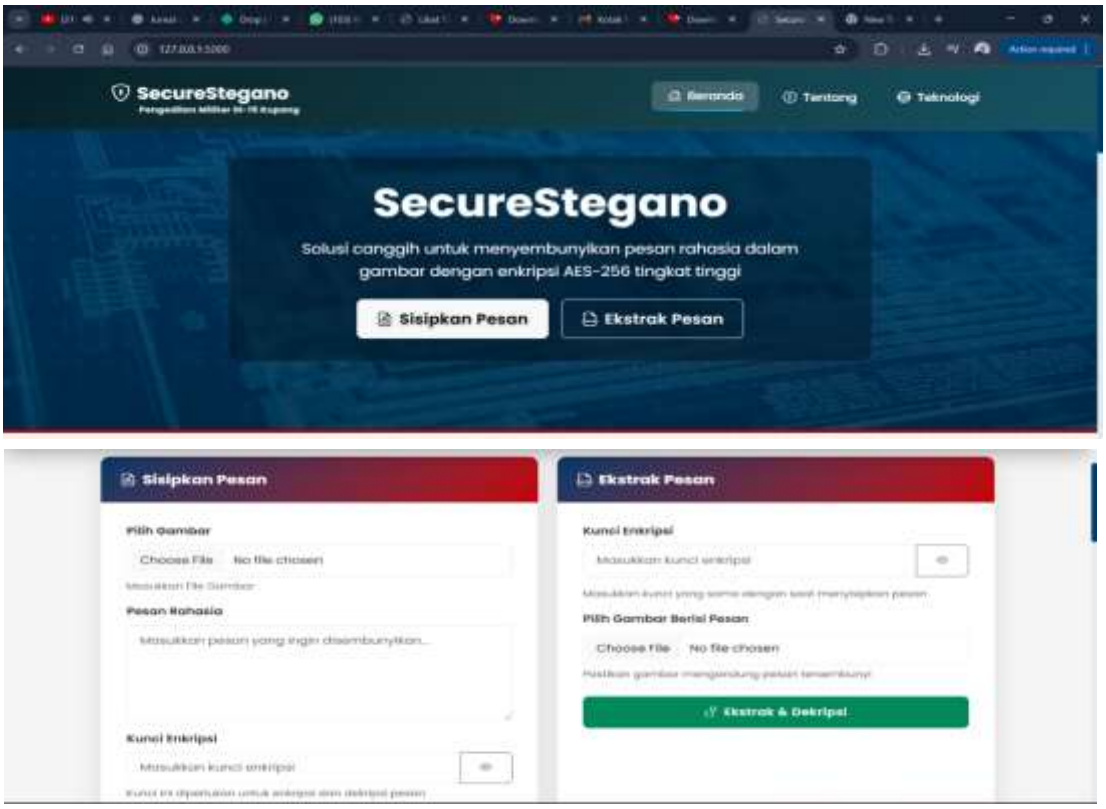
Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

4 Hasil dan Pembahasan (or Results and Analysis)

4.1 Implementasi Sistem

1. Halaman Utama

   Halaman utama merupakan tampilan awal sistem yang menyediakan dua fitur utama, yaitu penyisipan dan ekstraksi pesan rahasia. Pada fitur penyisipan, pengguna dapat mengunggah gambar, memasukkan pesan, serta menentukan kunci enkripsi untuk proses pengamanan pesan. Sementara itu, fitur ekstraksi memungkinkan pengguna mengunggah gambar yang telah disisipi pesan dan memasukkan kunci enkripsi untuk menampilkan kembali pesan rahasia yang tersembunyi di dalam gambar.



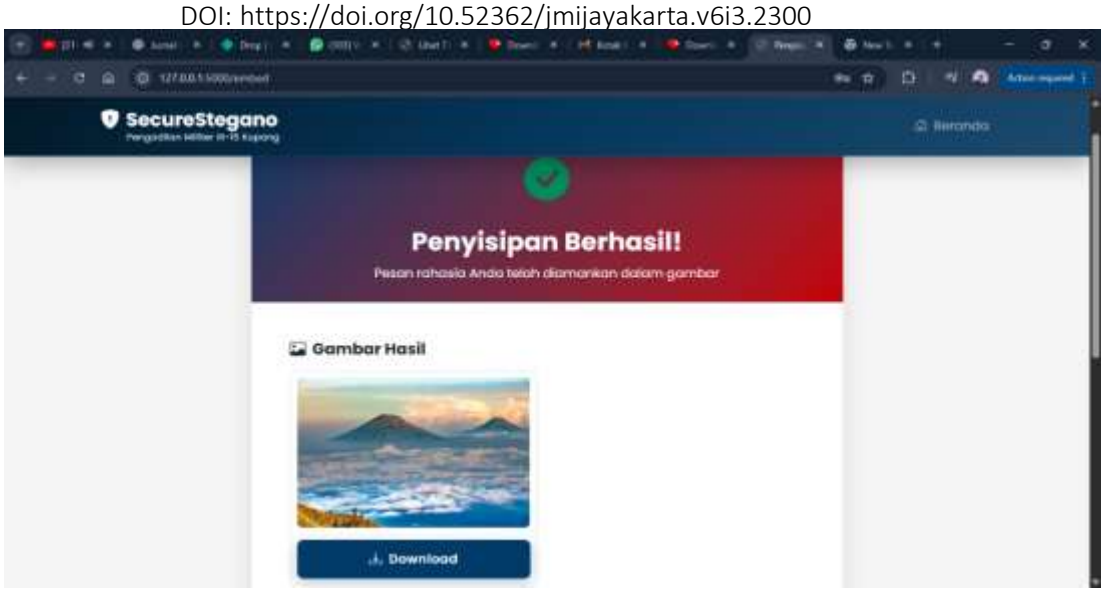
Gambar 4. Halaman Utama

2. Halaman *Embedding* Pesan

   Halaman *embedding* pesan menampilkan hasil citra digital yang telah berhasil disisipi pesan rahasia melalui proses enkripsi dan penyisipan. Pada halaman ini, pengguna dapat melihat *stego image* sebagai hasil akhir dari proses embedding. 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 yang tersedia pada halaman utama, sehingga pesan rahasia yang tersembunyi di dalam gambar dapat diekstrak dan ditampilkan kembali oleh sistem.

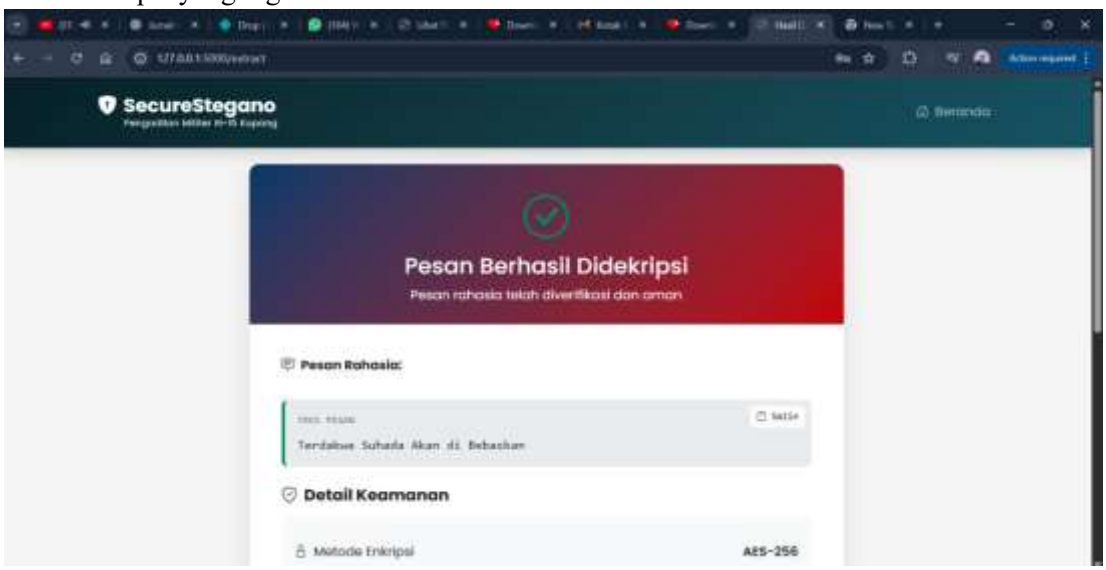
This work is licensed under a Creative Commons Attribution 4.0 International License.

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300



Gambar 5. Halaman Setelah *Embedding* Pesan

3. Halaman Dekripsi Pesan
   Halaman dekripsi pesan menampilkan hasil pesan asli (*plaintext*) yang berhasil diekstraksi dari gambar stego setelah melalui proses dekripsi. Tampilan ini muncul setelah pengguna melakukan ekstraksi pesan melalui form yang tersedia pada halaman utama. Melalui halaman ini, pengguna dapat melihat kembali isi pesan rahasia secara jelas dan aman sesuai dengan kunci enkripsi yang digunakan.



Gambar 6. Halaman Dekripsi Pesan

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

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

4.2 Pengujian Sistem

4.2.1. 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

4.2.2. 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.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

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

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

5 Kesimpulan (or Conclusion)

Penelitian ini berhasil mengembangkan sistem steganografi yang interaktif dan mudah digunakan untuk menyisipkan serta mengekstraksi pesan rahasia pada media gambar. Dengan mengombinasikan metode *Least Significant Bit* (LSB) dan algoritma kriptografi *Advanced Encryption Standard 256-bit* (AES-256), sistem ini mampu memberikan tingkat keamanan yang baik sekaligus mempertahankan kualitas visual gambar. Sistem yang dibangun memudahkan pengguna dalam melakukan proses penyisipan dan ekstraksi pesan melalui antarmuka yang sederhana dan fungsional.

Hasil penelitian menunjukkan bahwa sistem dapat bekerja secara efektif dan efisien, di mana pesan rahasia berhasil disembunyikan dan dikembalikan ke bentuk aslinya tanpa menimbulkan perubahan visual yang signifikan pada gambar. Diharapkan, sistem ini dapat menjadi solusi alternatif dalam pengamanan pesan digital berbasis steganografi, khususnya pada pertukaran informasi yang bersifat rahasia. Dengan demikian, pengembangan lebih lanjut dari sistem ini diharapkan dapat memberikan kontribusi positif dalam peningkatan keamanan data digital di masa mendatang.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta

Jurnal Manajemen Informatika Jayakarta
Volume 6, Nomor 3, September 2026: halaman 38-49
P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v6i3.2300

Referensi (Reference)

[1] L. Islami, H. P. Akbar, and R. G. Rizal, "Sistem Keamanan Informasi Di Era Digital," vol. 1, no. 11, pp. 1174–1177, 2024.

[2] M. A. Firdaus and A. Rahmatulloh, "Implementasi Steganografi Citra Digital Lsb Menggunakan Enkripsi Aes-256 Dan Embedding Pseudorandom," *J. Inform. dan Tek. Elektro Terap.*, vol. 13, no. 1, 2025, doi: 10.23960/jitet.v13i1.5620.

[3] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[4] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[5] R.M. Hilmy Hernandi and Joko Christian Chandra, "Implementasi Algoritme AES-256 dan AES-GCM untuk Mengamankan Dokumen Pada Sistem Data Rekam Medis Klinik Mulya," *KRESNA J. Ris. dan Pengabdi. Masy.*, vol. 4, no. 1, pp. 12–22, 2024, doi: 10.36080/kresna.v4i1.131.

[6] S. Festi, B. Jaya, S. M. Kuway, and G. Syarifudin, "Perancangan Perangkat Lunak Steganografi Menggunakan Least Significant Bit Dengan Enkripsi Vigenere Cipher," *e-Jurnal JUSITI (Jurnal Sist. Inf. dan Teknol. Informasi)*, vol. 9, no. 1, pp. 52–64, 2020, doi: 10.36774/jusiti.v9i1.643.

[7] A. Wisnu, Y. Prasetya, B. Suhardjo, and R. Munir, "Penggunaan Kombinasi Kriptografi Triple DES dan Teknik Steganografi LSB dalam Mengamankan Pesan Militer," *J. Sist. Inf. dan Teknol. Inf.*, vol. 12, no. 2, pp. 193–199, 2023.

[8] M. I. Kurniawan, E. Maryanto, and S. P. Rahayu, "Implementation of a Combination of Advanced Encryption Standard Cryptography With Subbytes Modification and Steganography Based on a Website," *J. Tek. Inform.*, vol. 5, no. 5, pp. 1375–1384, 2024, doi: 10.52436/1.jutif.2024.5.5.2665.

[9] M. Halim and Wulan Sri Lestari, "Steganography Menggunakan Advanced Encryption Standard dan Metode Least Significant Bit pada File Bitmap 24-bit," *J. Armada Inform.*, vol. 7, no. 2, pp. 295–300, 2023, doi: 10.36520/jai.v7i2.76.

This work is licensed under a Creative Commons Attribution 4.0 International License.
http://journal.stmikjayakarta.ac.id/index.php/JMIJayakarta