IMPLEMENTASI GABUNGAN AES-256 DAN RSA DENGAN METODE LSB UNTUK KEAMANAN DATA

Bintang Kusuma Ilham[1] **, Muhammad Fajar Sidiq**[2] **, M. Agung Nugroho**[2] **, Trihastuti Yuniati** [4]

[1,2,3,4] *Informatika Universitas Telkom*
email : bintangkusumailham@student.telkomuniversity.ac.id [1], *mfsidiq@telkomuniversity.ac.id* [2] , *magungnugroho@telkomuniversity.ac.id* [3] , *trihastutiy@telkomuniversity.ac.id* [4]

Abstraksi

Penelitian ini mengembangkan sistem keamanan data yang menggabungkan enkripsi ganda (AES-256 CBC dan RSA-2048) dengan steganografi *Least Significant Bit* (LSB) pada gambar PNG. Dibangun menggunakan Python dengan Tkinter, sistem ini menangani enkripsi/penyisipan, ekstraksi/dekripsi, dan evaluasi kinerja. Pengujian pada lima gambar PNG dengan ukuran teks bervariasi menunjukkan penyembunyian data yang berhasil. Rata-rata MSE adalah 0,0263730426 dan PSNR 64,3427895234 dB. Pesan asli berhasil dipulihkan sepenuhnya. Efisiensi sistem ditunjukkan oleh rata-rata waktu eksekusi 92,376 ms untuk enkripsi dan 370,392 ms untuk dekripsi, dengan penggunaan memori yang rendah. Kapasitas steganografi mendekati batas teoretis. Sistem ini terbukti efektif dalam mengamankan data teks dan memenuhi semua tujuan penelitian.

***Kata Kunci* :**
AES, Enkripsi, Kriptografi, RSA, Steganografi.

Abstract

This research presents a data security system that combines double encryption (AES-256 CBC and RSA-2048) with Least Significant Bit (LSB) steganography in PNG images. Developed in Python with Tkinter, it handles encryption/embedding, extraction/decryption, and performance evaluation. Testing on five PNG images with varying text sizes showed successful data concealment. The average MSE was 0.0263730426 and PSNR was 64.3427895234 dB. Original messages were fully recovered. The system's efficiency is highlighted by average execution times of 92.376 ms for encryption and 370.392 ms for decryption, with low memory usage. Steganographic capacity was near theoretical limits. This system effectively secures text data and achieves all research goals.

***Keywords* :**
Cryptography, Encryption, AES, RSA, Steganography.

Pendahuluan

Perkembangan teknologi informasi berperan penting sebagai sarana yang efisien dalam menciptakan serta meluaskan akses informasi, melalui pemanfaatan teknologi komputer dalam konteks bisnis [1]. Perkembangan teknologi informasi, ditandai dengan 5,4 miliar pengguna internet global pada 2023 telah mempercepat pertukaran informasi [2]. Namun, di balik kemajuan ini, ancaman keamanan data menjadi tantangan besar yang mengintai, karena data yang tidak terlindungi dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), sektor administrasi pemerintahan menjadi target utama serangan siber di Indonesia diikuti oleh sektor keuangan dan energi sepanjang tahun 2023 [3]. KumparanTECH juga menyoroti bahwa serangan siber di Indonesia pada semester pertama 2024 didominasi oleh pelaku dari dalam negeri [4]. Fenomena ini ditunjukkan pada Gambar 1, yang menggambarkan bahwa ancaman tidak hanya berasal dari luar, tetapi juga dari dalam negeri sendiri. Ancaman siber juga diperkirakan akan semakin berbahaya kedepannya [5].

Gambar 1. Distribusi Sumber Serangan Siber Ke Indonesia Pada Semester Pertama 2024 [4]

Salah satu teknik pengamanan data yang sering digunakan dan steganografi. Steganografi merupakan teknik pengamanan data yang menyembunyikan informasi sensitif ke dalam media digital sehingga

sulit dideteksi, namun sekaligus menimbulkan tantangan dalam analisis forensik digital [6]. Oleh karena itu, diperlukan pendekatan forensik yang andal untuk mendeteksi, memverifikasi, dan menjaga integritas data tersembunyi dalam proses investigasi. Perlindungan dari steganografi bisa lebih kuat dengan menambahkan teknik enkripsi kriptografi sebelum menyembunyikan pesan di dalam gambar [7]. Steganografi, di sisi lain, menyembunyikan data dalam media seperti gambar atau audio, sehingga keberadaan data tersebut tidak terdeteksi oleh pihak yang tidak berwenang [8]. Namun, pendekatan sebelumnya sering kali hanya menggunakan salah satu teknik, sehingga keamanan yang dihasilkan belum maksimal.

Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan solusi yang menggabungkan kriptografi dan steganografi untuk menciptakan sistem keamanan data yang lebih kuat. Pendekatan ini menggunakan algoritma *Advanced Encryption Standard* (AES), *Rivest Shamir Adleman* (RSA), dan metode *Least Significant Bit* (LSB). AES adalah algoritma kriptografi simetris yang menggunakan kunci dengan panjang tertentu dalam penelitian ini 256-bit untuk mengenkripsi data dalam blok berukuran 128-bit, dikenal karena kecepatan dan ketahanannya terhadap serangan seperti *brute force* [9] RSA adalah algoritma kriptografi asimetris yang memanfaatkan pasangan kunci publik dan privat dalam penelitian ini menggunakan kunci 2048-bit untuk mengamankan distribusi kunci dan memastikan hanya pihak yang berwenang yang dapat mengakses data [10]. Sementara itu, metode LSB menyisipkan data ke dalam bit paling tidak signifikan dari piksel gambar berwarna RGB, memungkinkan penyembunyian informasi tanpa mengubah tampilan visual gambar secara nyata, karena perubahan pada bit tersebut hanya menghasilkan perbedaan warna yang sangat kecil misalnya, dari nilai 255 menjadi 254 pada saluran warna [7]. Metode LSB dipilih untuk steganografi dalam penelitian ini karena kelebihannya dalam proses penyisipan dan ekstraksi yang cepat serta nilai MSE kecil dan PSNR besar, yang mendukung efisiensi dan ketahanan kualitas citra [8].

Pendekatan yang dilakukan penelitian ini adalah menerapkan teknik pengamanan data dengan model enkripsi yang berlapis, yang diharapkan dapat memberikan mekanisme tambahan pada pengamanan data. Dengan menerapkan Enkripsi AES-256 dan RSA-2048 memastikan data tidak dapat dibaca tanpa kunci, dan steganografi menyembunyikan keberadaan data tersebut, menjadikannya solusi yang lebih aman dibandingkan metode yang hanya menggunakan salah satu teknik. Data terenkripsi ini disembunyikan dalam gambar berwarna RGB (*.png) menggunakan metode LSB, menghasilkan gambar stego yang tampak identik dengan gambar asli. Format gambar PNG dipilih sebagai objek karena sifatnya yang lossless, memastikan integritas data LSB, berbeda dengan format JPEG yang dapat merusak data akibat kompresi *lossy* [7], [11].

Tinjauan Pustaka

Penelitian dengan implementasi sistem enkripsi data guna meningkatkan keamanan melalui kombinasi algoritma AES dan RSA. Penelitian ini memanfaatkan metode pengujian *black box* dan pembangkitan kunci 2048-bit, yang memakan waktu 495,56 ms, dengan hasil waktu enkripsi rata-rata AES sebesar 4,365 ms dan RSA 7,428 ms, serta waktu dekripsi AES 2,753 ms dan RSA 54,068 ms, menunjukkan efisiensi signifikan dalam proses ganda tersebut. Lebih lanjut, peneliti merekomendasikan pengembangan metode kombinasi yang lebih kompleks dan integrasi dengan media penyisipan seperti suara, video atau file berformat lainnya untuk memperluas cakupan keamanan data [12].

Salah satu Studi yang bertujuan merancang sistem kriptografi berbasis superenkripsi *Caesar Cipher* dan AES-128-EBC untuk mengamankan data pajak bumi dan bangunan (PBB) di tingkat desa. Penelitian ini menerapkan metode eksperimental dengan pengujian entropi, korelasi, dan *avalanche effect* pada 100 plainteks, menghasilkan korelasi rendah sebesar 0,257, entropi 5,75 (mendekati nilai maksimum 8), dan *avalanche effect* 11,30% (lebih baik dari AES tunggal 6,90%), menunjukkan peningkatan keamanan data terenkripsi. Seiring dengan itu, peneliti menyarankan perbandingan dengan metode lain seperti *Vigenere Cipher*, modifikasi AES-128-EBC untuk entropi lebih tinggi, dan penggunaan kunci dinamis untuk meningkatkan keamanan sistem [13].

Penelitian lain menciptakan aplikasi berbasis Android yang mengintegrasikan algoritma RC4 untuk kriptografi dan steganografi *Least Significant Bit* (LSB) guna mengamankan data rahasia. Studi ini mengadopsi metode studi pustaka, observasi, dan wawancara, dengan implementasi RC4 sebagai *stream cipher* menggunakan *S-Box* 256 byte dan LSB dengan penggantian bit terakhir pada gambar 24-bit. Hasil penelitian menunjukkan bahwa RC4 menghasilkan enkripsi yang efektif melalui *bit-wise-XOR*, sementara LSB berhasil menyisipkan file berformat *.docx, *.txt, *.xlsx, dan *.pdf tanpa perubahan visual signifikan, menawarkan solusi keamanan yang tidak mencurigakan. Lebih jauh, peneliti menyiratkan potensi pengembangan untuk meningkatkan kapasitas penyisipan atau mendukung jenis file lain, memperkuat aplikasi dalam konteks keamanan data mobile[14].

Kriptografi memiliki cabang salah satunya adalah steganografi yang dapat memungkinkan seseorang untuk menyimpan atau menyembunyikan informasi ke dalam bentuk gambar atau file lainnya. Steganografi dapat dikembangkan dengan merancang aplikasi desktop berbasis Java yang

mengintegrasikan AES-128 untuk enkripsi dan metode *End Of File* (EOF) untuk steganografi guna mengamankan data rahasia di Dinas Pendidikan Kabupaten Tangerang. Penelitian ini menerapkan transformasi AES-128 (*SubBytes, ShiftRows, MixColumns, AddRoundKey*) pada 10 putaran dan penyisipan data di akhir file gambar, dengan pengujian pada berbagai file (*.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, *.pdf, *.txt, *.jpg, *.png). Hasil penelitian menunjukkan keberhasilan enkripsi-dekripsi yang meningkatkan keamanan ganda, meskipun waktu proses lama pada file besar dan ukuran file terenkripsi meningkat. Sejalan dengan itu, peneliti merekomendasikan peningkatan kinerja enkripsi untuk file besar, dukungan file lain, dan penggunaan algoritma kompresi untuk mengurangi ukuran file [14].

Dalam penelitian yang menganalisis sistem steganografi citra menggunakan metode *Least Significant Bit* (LSB) dengan MATLAB untuk menyembunyikan data rahasia, dengan evaluasi berdasarkan *Peak Signal to Noise Ratio* (PSNR), waktu proses, dan ukuran file. Studi ini mengimplementasikan LSB pada gambar PNG32 dengan konversi ASCII, melibatkan pengujian pada 10 file gambar batik Bentenan bervariasi ukuran dan resolusi menggunakan GUI MATLAB. Hasil penelitian menunjukkan PSNR tinggi (63,785–63,965 untuk Gambar 1, 54,799–55,196 untuk Gambar 2), mengindikasikan derau minimal, serta MSE rendah (0,034–0,035 untuk Gambar 1, 0,198–0,217 untuk Gambar 2), menegaskan kualitas stego yang baik, dengan waktu proses meningkat seiring panjang teks (7,5–64,6 detik untuk Gambar 1, 6,3–61,9 detik untuk Gambar 2) dan ekstraksi teks valid hingga 30.000 karakter. Sejalan dengan itu, peneliti menyarankan perhatian pada ukuran citra [15].

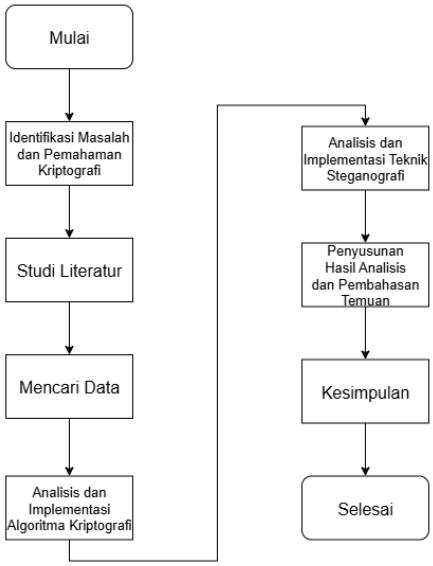
Untuk analisis pengaruh variabel citra terhadap kombinasi kriptografi RSA dan steganografi LSB dalam pengamanan pesan, dengan evaluasi kualitas citra menggunakan PSNR, MSE, NCC, dan SSIM. Studi ini mengimplementasikan RSA dengan bilangan prima dan LSB pada citra berformat BMP, PNG, TIFF, JPG dengan ukuran 64×64 hingga 1024×1024 piksel, melibatkan pengujian penyisipan teks bervariasi panjang (336–149360 bit). Hasil penelitian menunjukkan citra kecil (64×64, 128×128) gagal menyisipkan pesan panjang, sedangkan citra besar (512×512, 1024×1024) berhasil, dengan MSE tertinggi 0,034150413 (128×128) dan terendah 0,004282579 (1024×1024), PSNR 23,163125–79,96560625 dB, serta NCC dan SSIM mendekati 1 pada citra besar, menegaskan kemiripan tinggi. Lebih jauh, peneliti merekomendasikan penambahan parameter pengujian seperti steganalysis untuk meningkatkan keamanan sistem [7].

Analisis kriptografi dapat dikembangkan dalam bentuk sistem. Salah satunya mengintegrasikan algoritma kriptografi RSA dan El-Gamal dengan steganografi LSB untuk mengamankan data. Studi ini menggunakan metode *black-box* testing untuk validasi fungsionalitas sistem, dengan pengujian pada file .docx sebagai pesan rahasia dan file audio .wav sebagai media penutup. Hasil penelitian menunjukkan bahwa RSA lebih cepat dalam proses enkripsi, sedangkan El-Gamal unggul dalam dekripsi, dengan nilai PSNR berkisar antara 59.87-67.69 dB untuk stego audio, menunjukkan kualitas audio yang baik. Pengujian BER menunjukkan nilai 0, menegaskan integritas data terjaga. Peneliti merekomendasikan penyesuaian algoritma berdasarkan kebutuhan spesifik sistem [16].

Penerapan kriptografi AES-128 dengan steganografi *Spread Spectrum* dapat mengamankan data teks dalam gambar [17]. Studi ini melibatkan proses enkripsi AES dengan tahapan seperti *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*, diikuti penyisipan *ciphertext* ke gambar *.png menggunakan *Spread Spectrum*. Hasil pengujian menunjukkan MSE rendah dan PSNR di atas 30 dB, menandakan kualitas gambar stego tetap baik, dengan ketahanan terhadap noise. Peneliti menyimpulkan bahwa kombinasi ini efektif untuk keamanan data, meskipun waktu pemrosesan lebih lama dibandingkan metode sederhana [18].

Metode Penelitian

Dalam menyusun laporan penelitian ini terdapat beberapa tahap dalam melakukan penelitian. Proses penelitian meliputi langkah-langkah berikut:



Gambar . Diagram Alir Penelitian

1. Identifikasi Masalah dan Pemahaman Kriptografi

Pada tahap awal penelitian ini, fokus utama adalah mengidentifikasi masalah yang ada dalam keamanan data digital, terutama dalam konteks pengiriman data sensitif melalui media digital.

2. Studi Literatur

Tahap ini melibatkan pengumpulan referensi dari jurnal dan artikel terkait untuk membangun dasar teoretis penelitian. Literatur yang dikaji mencakup implementasi AES, RSA, dan LSB, serta metrik evaluasi.

3. Mencari Data

Proses pengumpulan data dilakukan dengan memilih sampel teks dalam format *.txt dan gambar berwarna format *.png sebagai media steganografi. Data dikumpulkan dari sumber internal, seperti file uji coba, dan diolah untuk memastikan kesesuaian dengan kebutuhan enkripsi dan penyisipan, yang telah diuji pada berbagai resolusi gambar.

4. Analisis dan Implementasi Algoritma Kriptografi

Tahap ini melibatkan integrasi algoritma AES-256 mode CBC dan RSA-2048 untuk mengamankan data teks. Proses dimulai dengan pembangkitan *secret key* acak 256-bit untuk mengenkripsi teks asli menjadi *ciphertext* menggunakan AES-256. *Secret key* tersebut kemudian dienkripsi dengan kunci publik RSA-2048 untuk menambah lapisan keamanan. Proses enkripsi AES melibatkan transformasi *SubBytes, ShiftRows, MixColumns,* dan *AddRoundKey* selama 14 putaran, dengan vektor inisialisasi (IV) untuk mengacak blok pertama. Untuk dekripsi, data diekstrak dari gambar stego menggunakan metode LSB, *secret key* didekripsi dengan kunci privat RSA, dan *ciphertext* didekripsi dengan AES-256 untuk memulihkan teks asli.

5. Analisis dan Implementasi Teknik Steganografi

Tahap ini melibatkan penyisipan *ciphertext* ke dalam gambar berwarna format PNG menggunakan metode *Least Significant Bit* (LSB). Proses dimulai dengan mengambil *ciphertext* dan gambar *cover*, lalu mengonversi *ciphertext* ke kode ASCII dan representasi biner. Nilai piksel gambar juga dikonversi ke biner, di mana bit terakhir (LSB) dari setiap saluran warna (R, G, B) diganti dengan bit pesan secara berurutan. Setelah penyisipan selesai, data biner dikonversi kembali ke piksel, menghasilkan gambar stego yang tampak identik dengan gambar asli.

6. Penyusunan Hasil Analisis dan Pembahasan Temuan

Pada tahap ini, hasil dari implementasi steganografi dengan enkripsi menggunakan algoritma AES dan RSA akan dianalisis secara menyeluruh.

7. Kesimpulan

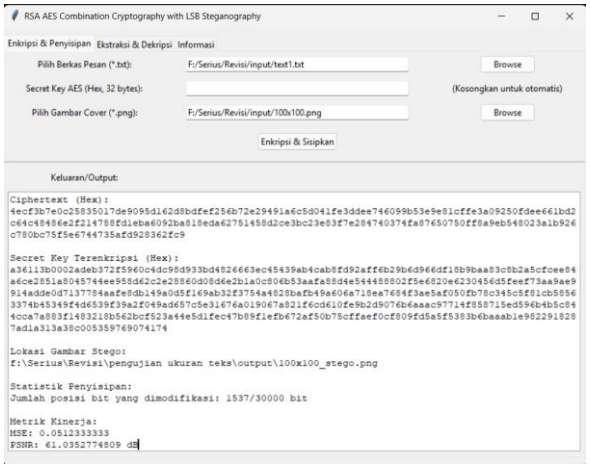
Bagian ini merangkum hasil analisis dan implementasi untuk menilai efektivitas sistem keamanan data. Berdasarkan data yang telah diperoleh, kesimpulan menegaskan keunggulan kombinasi AES-256, RSA-2048, dan LSB, berdasarkan pengujian yang dilakukan.

Hasil dan Pembahasan

Hasil dari pengembangan sistem keamanan data berbasis kombinasi algoritma AES-256, RSA-2048, dan steganografi LSB pada gambar berwarna format PNG. Hasil tersebut mencakup pengembangan aplikasi, pengujian yang dilakukan terhadap fungsi enkripsi/penyisipan dan ekstraksi/dekripsi, serta analisis terhadap kinerja sistem berdasarkan metrik MSE, PSNR, waktu eksekusi, penggunaan memori, dan kapasitas steganografi.

1. Implementasi

Sistem keamanan data dikembangkan menggunakan Python dengan antarmuka Tkinter pada laptop dengan spesifikasi Intel Core i5-13450HX, RAM 24 GB, dan Windows 11. Sistem mencakup tiga fungsi utama: enkripsi/penyisipan, ekstraksi/dekripsi, dan pengukuran performa, diimplementasikan melalui tiga tab antarmuka. Berikut adalah hasil dari pengembangan sistem keamanan data berbasis kombinasi algoritma AES-256, RSA-2048, dan steganografi LSB yang tersaji pada gambar 3.



Gambar 2. *Screenshot* Antarmuka Tab "Enkripsi & Penyisipan"

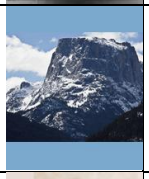
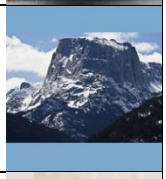
2. Hasil

Pengujian dilakukan pada lima gambar PNG (100x100 hingga 500x500 piksel) dengan pesan teks 388–2948 *byte*, menghasilkan data visual, enkripsi, penyisipan, kualitas gambar, waktu eksekusi, penggunaan memori, ukuran file, dan status ekstraksi/dekripsi.

a. Perbandingan Visual Gambar Asli dan Gambar Stego

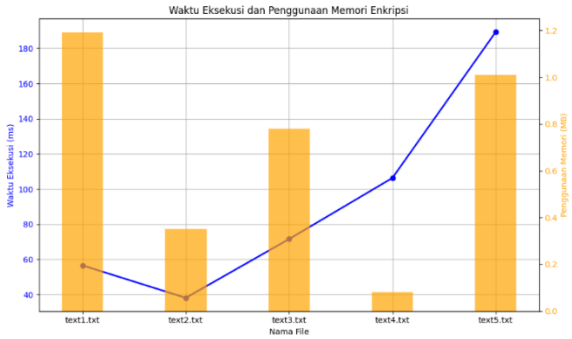
Pada tabel 1 menunjukkan pasangan gambar asli dan stego untuk setiap resolusi yang digunakan dalam percobaan.

Tabel 1. Perbandingan Visual Gambar Asli Dan Gambar Stego

Nama Gambar Penampung	Resolusi	Gambar Asli	Gambar Stego
100x100.png	100x100 px		
200x200.png	200x200 px		
300x300.png	300x300 px		
400x400.png	400x400 px		
500x500.png	500x500 px		

b. Hasil Enkripsi

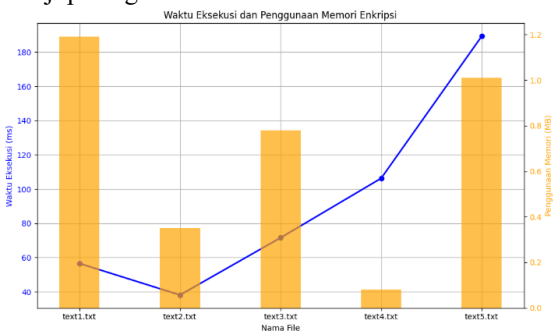
Grafik garis biru yang menggambarkan waktu eksekusi dan grafik batang oranye yang menunjukkan penggunaan memori untuk lima file teks. Garis biru mengindikasikan kenaikan waktu eksekusi dari 56.58 ms ke 189.31 ms, mencerminkan pengaruh ukuran pesan terhadap enkripsi AES-256 dan RSA-2048. Proses ini tersaji pada gambar 6.



Gambar 3. Grafik Waktu Eksekusi Dan Penggunaan Memori Enkripsi

c. Hasil Penyisipan

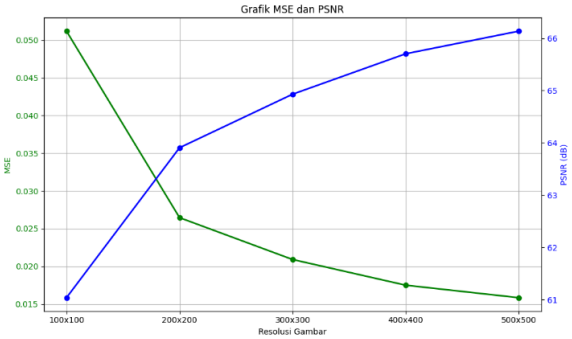
Grafik batang oranye yang menggambarkan jumlah bit yang diubah dan grafik garis biru yang menunjukkan persentase bit yang diubah berdasarkan resolusi gambar. Batang oranye menggambarkan peningkatan jumlah bit yang diubah seiring bertambahnya ukuran data, menunjukkan kapasitas penyisipan yang meningkat. Garis biru menunjukkan penurunan persentase bit yang diubah. Karena total bit yang lebih besar, menegaskan efisiensi metode LSB pada gambar dengan resolusi tinggi. Proses ini tersaji pada gambar 7.



Gambar 4. Grafik Jumlah Bit Yang Diubah Dan Persentase

d. Hasil Pengujian Kualitas Gambar (MSE dan PSNR)

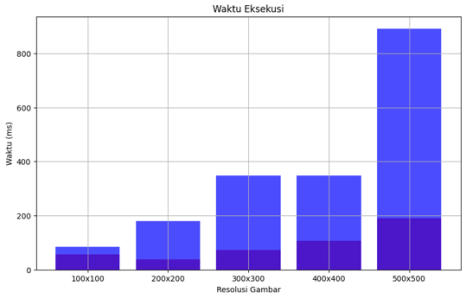
Grafik garis hijau yang menggambarkan MSE dan grafik garis biru yang menunjukkan PSNR berdasarkan lima resolusi gambar. Garis hijau menunjukkan penurunan MSE seiring meningkatnya resolusi, mengindikasikan perbedaan piksel yang semakin kecil. Garis biru menunjukkan kenaikan PSNR, menandakan kualitas gambar stego yang sangat baik dengan perubahan visual yang hampir tak terlihat. Proses ini tersaji pada gambar 8.



Gambar 5. Grafik MSE dan PSNR

e. Hasil Pengujian Waktu Eksekusi

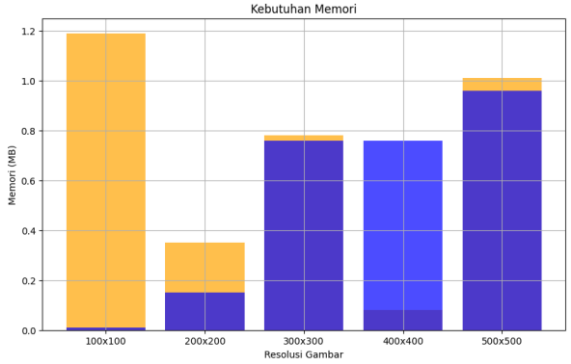
Grafik batang merah yang menggambarkan waktu enkripsi dan penyisipan serta grafik batang biru yang menunjukkan waktu ekstraksi dan dekripsi berdasarkan resolusi gambar. Batang merah menunjukkan peningkatan waktu enkripsi dan penyisipan, dipengaruhi oleh ukuran data dan resolusi. Batang biru menunjukkan kenaikan waktu ekstraksi dan dekripsi, mencerminkan kompleksitas dekripsi RSA pada data besar. Hasil ini tersaji pada gambar 9.



Gambar 6. Grafik Waktu Eksekusi

f. Hasil Pengujian Kebutuhan Memori

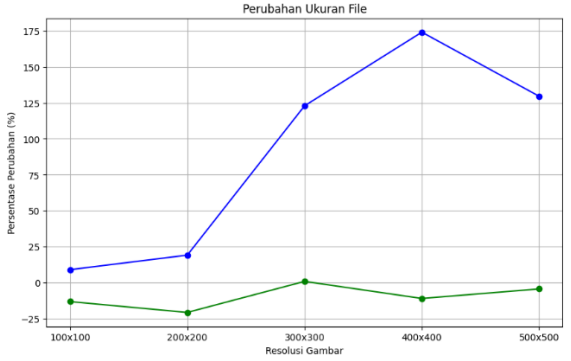
Grafik batang oranye yang menggambarkan kebutuhan memori enkripsi dan penyisipan serta grafik batang biru yang menunjukkan kebutuhan memori ekstraksi dan dekripsi berdasarkan resolusi gambar. Batang oranye menunjukkan variasi kebutuhan memori enkripsi dan penyisipan. Batang biru menunjukkan peningkatan kebutuhan memori ekstraksi dan dekripsi. Hasil ini tersaji pada gambar 10.



Gambar 7. Grafik Kebutuhan Memori

g. Hasil Pengujian Ukuran File

Grafik garis hijau yang menggambarkan persentase perubahan ukuran tanpa kodingan *compress_level=0* dan grafik garis biru yang menunjukkan persentase perubahan dengan kodingan *compress_level=0*. Garis hijau menunjukkan variasi persentase perubahan tanpa kodingan, dengan penurunan, akibat kompresi otomatis *DEFLATE* oleh pustaka Pillow. Proses ini tersaji pada gambar 11.



Gambar 8. Grafik Peerubahan ukuran File

h. Status Keberhasilan Ekstraksi dan Dekripsi

Untuk memastikan keandalan sistem, status keberhasilan proses ekstraksi dan dekripsi juga dicatat. Hasilnya ditunjukkan pada tabel 2.

Tabel 2. Status Keberhasilan Ekstraksi Dan Dekripsi

Nama Gambar Stego	**Resolusi**	**Status Ekstraksi dan Dekripsi**	**Nama Gambar Stego**
100x100_stego.png	100x100 px	Berhasil	100x100_stego.png
200x200_stego.png	200x200 px	Berhasil	200x200_stego.png
300x300_stego.png	300x300 px	Berhasil	300x300_stego.png
400x400_stego.png	400x400 px	Berhasil	400x400_stego.png
500x500_stego.png	500x500 px	Berhasil	500x500_stego.png

Hasil menunjukkan bahwa proses ekstraksi dan dekripsi berhasil untuk semua gambar stego tanpa kehilangan informasi. Pesan asli dapat dikembalikan dengan sempurna, yang menunjukkan bahwa sistem ini dapat diandalkan untuk menjaga integritas data.

3. Analisis

Analisis dilakukan untuk mengevaluasi kinerja sistem keamanan data berbasis kombinasi AES-256, RSA-2048, dan steganografi LSB. Analisis ini mencakup penilaian kualitas gambar stego, efisiensi performa sistem, dampak ukuran file stego, dan kapasitas steganografi berdasarkan pengujian pada lima gambar.

a. Analisis Kualitas Gambar Stego (MSE dan PSNR)

Hasil analisis menunjukkan rata-rata MSE 0,0263730426 dan PSNR 64,3427895234 dB, mengindikasikan perbedaan piksel minimal antara gambar asli dan stego. Nilai MSE rendah dan PSNR tinggi (>30 dB) memastikan kualitas gambar stego sangat baik, dengan perubahan visual hampir tidak terdeteksi, mendukung efektivitas metode LSB.

b. Analisis Efisiensi Performa Sistem (Waktu Eksekusi dan Kebutuhan Memori)

Rata-rata waktu eksekusi enkripsi/penyisipan 92,376 ms dan ekstraksi/dekripsi 370,392 ms, dengan dekripsi lebih lambat akibat kompleksitas RSA-2048. Rata-rata penggunaan memori 0,682 MB (enkripsi) dan 0,528 MB (dekripsi) menunjukkan efisiensi baik

untuk skala kecil hingga menengah, meskipun performa dekripsi menurun pada resolusi tinggi.

c. Analisis Ukuran File Stego

Rata-rata perubahan ukuran file stego tanpa *compress_level=0* adalah -9,63%, akibat kompresi otomatis DEFLATE oleh pustaka Pillow. Dengan *compress_level=0*, ukuran file meningkat 90,944% (puncak 174,06% pada 400x400 px), mencerminkan penambahan data terenkripsi (panjang *secret key*, *secret key* terenkripsi, IV, *ciphertext*), sesuai logika steganografi.

d. Analisis Ukuran File Stego

Kapasitas praktis (93.354 karakter pada 500x500 px) mendekati teoretis (93.746 karakter), dengan selisih 295–395 karakter pada resolusi rendah akibat *overhead metadata* (panjang *secret key* terenkripsi, *secret key* terenkripsi, IV). Selisih mengecil pada resolusi tinggi, menunjukkan efisiensi penyisipan LSB.

Kesimpulan dan Saran

Penelitian ini berhasil mengembangkan sistem keamanan data yang mengintegrasikan enkripsi ganda menggunakan algoritma AES-256 mode Cipher Block Chaining (CBC) dan RSA-2048 dengan steganografi Least Significant Bit (LSB) pada gambar berwarna format PNG, memenuhi ketiga tujuan penelitian yang ditetapkan pada Bab 1. Sistem yang dibangun menggunakan Python dengan antarmuka Tkinter mampu mengenkripsi data teks (*.txt) dengan AES-256 dan RSA-2048, menyembunyikannya ke dalam gambar PNG menggunakan metode LSB, serta memulihkan pesan asli tanpa kehilangan data.

Kualitas gambar stego menunjukkan rata-rata Mean Squared Error (MSE) 0,0263730426 dan Peak Signal-to-Noise Ratio (PSNR) 64,3427895234 dB, mengindikasikan perubahan visual minimal yang memastikan imperceptibility tinggi. Efisiensi sistem ditunjukkan oleh rata-rata waktu eksekusi 92,376 ms untuk enkripsi/penyisipan dan 370,392 ms untuk ekstraksi/dekripsi, serta penggunaan memori 0,682 MB dan 0,528. Analisis dimensi gambar menunjukkan bahwa kapasitas steganografi mendekati batas teoretis (misalnya, 93.354 karakter praktis dan 93.746 karakter teoretis pada 500x500 px), dengan selisih kapasitas (295-395 karakter) lebih signifikan pada resolusi rendah. Penggunaan parameter *compress_level=0* memastikan ukuran file stego meningkat sesuai data yang disisipkan (rata-rata perubahan 90,944%), mendukung keandalan steganografi. Dengan demikian, sistem ini terbukti efektif dalam mengamankan data teks dengan keamanan tinggi, kualitas visual yang sangat baik, efisiensi memadai, dan kapasitas optimal yang dipengaruhi dimensi gambar, sehingga mencapai semua tujuan penelitian.

Berdasarkan hasil penelitian dan analisis, berikut adalah beberapa saran untuk pengembangan lebih lanjut agar sistem ini dapat lebih baik :

1. Mengoptimalisasi Waktu Eksekusi ekstraksi/dekripsi yang meningkat pada resolusi tinggi akibat kompleksitas RSA-2048.
2. Pengujian pada Beragam Format Gambar seperti JPEG atau BMP serta mengidentifikasi kelemahan terkait kompresi *lossy* dan memastikan robustitas metode LSB terhadap variasi format.
3. Integrasi Metode Steganografi Lain untuk mengatasi kelemahan LSB sekuensial yang rentan terhadap analisis statistik, metode lain dapat diintegrasikan untuk meningkatkan keamanan dan kapasitas.

Daftar Pustaka

[1] I. Y. Sari *et al.*, *Keamanan Data dan Informasi*. Yayasan Kita Menulis, 2020.

[2] International Telecommunication Union, *Measuring digital development facts and figures 2023 - Penelusuran Google*. ITUPublications, 2023. Accessed: Jan. 06, 2026. [Online]. Available: https://www.itu.int/itu-d/reports/statistics/wp-content/uploads/sites/5/2023/11/Measuring-digital-development-Facts-and-figures-2023-E.pdf

[3] A. Ahdiat, "Pemerintahan, Sektor Paling Rentan Insiden Siber," Katadata. Accessed: Jan. 06, 2026. [Online]. Available: https://databoks.katadata.co.id/infografik/2024/07/02/pemerintahan-sektor-paling-rentan-insiden-siber

[4] kumparanTECH, "Serangan Siber ke Indonesia Banyak Berasal dari Dalam Negeri." Accessed: Jan. 06, 2026. [Online]. Available: https://kumparan.com/kumparantech/awanpintar-id-serangan-siber-ke-indonesia-banyak-berasal-dari-dalam-negeri-2273mCjMVDr

[5] J. M. Gultom, "Implementasi Algoritma Rsa Dan Algoritma Vernam Cipher Untuk Keamanan Data Pegawai Dinas Lingkungan Hidup," *J. DEVICE*, vol. 11, no. 2, pp. 30–38, 2021.

[6] N. D. Arizona, M. A. Nugroho, A. R. Syujak, R. K. Saputra, and I. Sulistyowati, "Metadata Forensic Analysis as Support for Digital Investigation Process by Utilizing Metadata-Extractor," *J. Intell. Softw. Syst.*, vol. 3, no. 2, pp. 27–31, 2024.

[7] A. R. Mido and E. I. H. Ujianto, "Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB," *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 9, no. 2, p. 279, Feb. 2022, doi: 10.25126/jtiik.2022914852.

[8] A. P. Ratnasari and F. A. Dwiyanto, "Metode steganografi citra digital," *Sains Apl*

Komputasi Dan Teknol Inf, vol. 2, no. 2, p. 52, 2020.

[9] M. Rizki and P. F. Ariyani, "Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal," *SKANIKA Sist. Komput. Dan Tek. Inform.*, vol. 4, no. 2, pp. 77–82, 2021.

[10] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," *KOMIK Konf.*, vol. 4, pp. 78–86, 2020.

[11] B. K. Yakti and R. H. Prayitno, "Perbandingan Dan Analisa Gambar Pada Steganografi Berdasarkan MSE Dan PSNR," *ICIT J.*, vol. 6, no. 2, pp. 138–152, Aug. 2020, doi: 10.33050/icit.v6i2.1105.

[12] A. Hermawan and E. I. H. Ujianto, "Implementasi Enkripsi Data Menggunakan Kombinasi AES Dan RSA," *InfoTekJar J. Nas. Inform. Dan Teknol. Jar.*, vol. 5, no. 2, pp. 325–330, Mar. 2021, doi: 10.30743/infotekjar.v5i2.3585.

[13] N. Ratama and M. Munawaroh, "Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android," *J. MEDIA Inform. BUDIDARMA*, vol. 6, no. 2, p. 1272, Apr. 2022, doi: 10.30865/mib.v6i2.3902.

[14] A. E. Putri, A. Kartikadewi, and L. A. A. Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag. AISM*, vol. 3, no. 2, pp. 69–78, 2020, doi: 10.15408/aism.v3i2.14722.

[15] V. Veriarinal and R. Wanandi, "IMPLEMENTASI SISTEM STEGANOGRAFI CITRA DENGAN METODE SUBTITUSI LSB (LEAST SIGNIFICANT BIT)," *Kohesi J. Sains Dan Teknol.*, vol. 2, no. 11, pp. 10–20, Mar. 2024, doi: 10.3785/kohesi.v2i11.2674.

[16] N. A. Fauzi, W. A. Prabowo, and A. J. T. Segara, "Analisis pengembangan aplikasi menggunakan algoritma RSA dan El-Gamal pada teknik steganografi dengan metode Least Significant Bit (LSB)," *E-Proceeding Eng.*, vol. 2, no. 12, 2025.

[17] S. F. R. Salsabila, A. I. Hadiana, and F. R. Umbara, "Penerapan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Spread Spectrum Untuk Mengamankan Pesan Dalam Gambar," *J. Inform. Commun. Technol. JICT*, vol. 5, no. 2, pp. 196–209, Dec. 2023, doi: 10.52661/j_ict.v5i2.216.

[18] D. Z. Berliani and T. Yuniati, "Penerapan kriptografi AES dan steganografi gambar dengan metode Spread Spectrum untuk pengaman data teks," *E-Proceeding Eng.*, vol. 12, no. 2, pp. 3406–3412, 2023.