PENERAPAN KRIPTOGRAFI AES DAN STEGANOGRAFI GAMBAR DENGAN METODE *SPREAD SPECTRUM* UNTUK PENGAMAN DATA TEKS

1st Diva Zahra Berliani
Telkom University Purwokerto
Purwokerto, Jawa Tengah
divazahraa@student.telkomuniversity.ac.id

2nd Trihastuti Yuniati
Telkom University Purwokerto
Purwokerto, Jawa Tengah
trihastutiy@telkomuniversity.ac.id

***Abstrak* — Keamanan data menjadi salah satu aspek penting di era digital, terutama dalam perlindungan informasi sensitif terhadap ancaman peretasan dan pencurian data. Salah satu tantangan utama adalah bagaimana menjaga kerahasiaan dan integritas data saat dikirim melalui jaringan yang rentan terhadap serangan. Untuk mengatasi masalah ini, penelitian ini mengusulkan solusi dengan mengombinasikan algoritma Advanced Encryption Standard (AES) 128-bit sebagai metode enkripsi data dan teknik steganografi Spread Spectrum untuk menyisipkan ciphertext ke dalam gambar. Menyisipkan Ciphertext ke dalam gambar menggunakan teknik Spread Spectrum membantu menjaga kerahasiaan dan integritas data karena pesan yang telah dienkripsi tersembunyi di dalam gambar yang terlihat seperti gambar biasa,sehingga mengurangi risiko deteksi oleh pihak yang tidak berwenang. Hal ini meningkatkan keamanan data yang dikirimkan karena ciphertext tersebar di seluruh gambar. Tujuan penelitian ini adalah untuk mengimplementasikan metode AES (Advanced Encryption Standard) untuk enkripsi dan Steganografi Spread Spectrum untuk penyisipan ciphertext ke dalam gambar, serta menguji efektivitasnya dalam menjaga kualitas gambar dan keamanan data. Hasil pengujian menunjukkan bahwa metode ini dapat menjaga kerahasiaan dan integritas data dengan baik, dengan nilai Mean Square Error (MSE) yang berada dalam kisaran rendah dan Peak Signal-to-Noise Ratio (PSNR) di atas 30 dB, yang menandakan kualitas gambar tetap baik setelah penyisipan pesan. Dengan demikian, kombinasi AES dan Spread Spectrum dapat menjadi solusi potensial untuk perlindungan data dalam berbagai aplikasi keamanan informasi.**

***Kata kunci*— AES, Spread Spectrum, Steganografi, Keamanan Data, MSE, PSNR.**

I. PENDAHULUAN

Kemajuan teknologi perangkat lunak semakin pesat dan mahal karena perubahan persyaratan yang cepat dan pengenalan teknologi baru [1]. Untuk pengembangan atau pemeliharaan perangkat lunak, tidak cukup hanya melindunginya, tetapi perlu menemukan cara yang lebih canggih untuk perlindungan [2]. Teknologi informasi saat ini lebih maju dibandingkan masa lalu yang masih memiliki banyak kekurangan [3]. Kemajuan teknologi ini memungkinkan manusia meningkatkan kualitas hidup dengan memanfaatkan teknologi untuk memenuhi kebutuhan, menciptakan nilai baru dalam kehidupan sosial, dan mendorong perkembangan manusia [4]. Teknologi modern memungkinkan manusia menggunakan jaringan yang sangat cepat untuk mencari informasi secara daring. Jaringan internet yang sebelumnya menggunakan 4G kini telah ditingkatkan menjadi 5G, yang kecepatannya hingga 20 kali lipat lebih cepat dari 4G. Bahkan, jaringan 6G sedang dipersiapkan untuk masa depan [5]. Seiring dengan kemajuan teknologi, keamanan juga harus ditingkatkan untuk melindungi dari serangan kejahatan di internet. Peningkatan penggunaan teknologi dan internet juga berdampak pada meningkatnya kejahatan daring oleh individu yang tidak bertanggung jawab untuk keuntungan pribadi. Salah satu bentuk kejahatan dunia maya adalah phishing [6]. Phishing adalah tindakan kriminal di internet yang bertujuan mencuri informasi pribadi korban. Kegiatan phishing dilakukan dengan tujuan mendapatkan informasi rahasia pengguna melalui email dan situs web palsu yang menyerupai situs web resmi[7]. Informasi yang dicari pelaku phishing mencakup kata sandi akun atau nomor kartu kredit. Email sering menjadi media utama untuk kegiatan phishing. Sebagai alat penting pertukaran informasi, email diperlukan oleh individu maupun lembaga. Dalam pertukaran informasi, sering terjadi pertukaran data sensitif yang memerlukan perlindungan. Untuk menjaga keamanan pesan yang dikirim, enkripsi digunakan untuk mengamankan data digital sehingga tidak dapat dipahami oleh pihak yang tidak berwenang [8]. Dalam konteks keamanan lampiran email, teknologi yang dapat digunakan mencakup lapisan transport yang menggunakan algoritma seperti Advanced Encryption Standard (AES) dan Spread Spectrum [9]. Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris yang diperkenalkan oleh National Institute of Standards and Technology (NIST) pada tahun 2001. AES menggantikan algoritma enkripsi sebelumnya, Data Encryption Standard (DES). Algoritma ini memiliki tiga variasi, yaitu AES-128, AES-192, dan AES-256, yang masing-masing memiliki panjang kunci yang berbeda. Semakin panjang kunci, semakin tinggi tingkat keamanannya [10]. Proses enkripsi AES melibatkan beberapa

tahap, termasuk SubBytes (penggantian byte), ShiftRows (pergeseran baris), MixColumns (penggabungan kolom), dan AddRoundKey (penambahan kunci putaran). Setiap langkah diulang dalam beberapa putaran, tergantung pada panjang kunci yang digunakan [11]. Sementara itu, Spread Spectrum adalah metode transmisi yang menggunakan kode pseudo noise untuk menyebar energi sinyal dalam jalur komunikasi. Penerima akan mengumpulkan kembali sinyal menggunakan replikasi kode pseudo noise yang disinkronkan [12]. Dalam konteks steganografi, teknik Spread Spectrum menambahkan derau semu (pseudo noise) ke objek penutup. Karena karakteristiknya mirip dengan noise, spread spectrum sulit dideteksi, diinterferensi, atau dimanipulasi [13]. Masalah yang dihadapi dalam penelitian ini adalah bagaimana menjaga keamanan dan kerahasiaan data teks saat dikirim melalui jaringan yang rentan terhadap serangan. Data yang dienkripsi menggunakan metode kriptografi saja masih dapat menarik perhatian pihak yang tidak berwenang, sehingga diperlukan teknik tambahan untuk menyembunyikan keberadaan data tersebut agar tidak mudah dideteksi [14]. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan kombinasi kriptografi AES dan steganografi Spread Spectrum dalam pengamanan data teks pada media gambar. Selain itu, penelitian ini juga bertujuan untuk menganalisis efektivitas metode yang digunakan dalam menjaga kualitas gambar setelah penyisipan pesan, dengan mengukur Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR). Dengan metode ini, diharapkan data yang dikirim tidak hanya terenkripsi dengan aman tetapi juga tersembunyi dengan baik dalam media gambar, sehingga sulit dideteksi oleh pihak yang tidak berwenang.

II. KAJIAN TEORI

Kajian teori ini menyajikan dan menjelaskan teori-teori yang berkaitan dengan variabel penelitian sebagai dasar dalam pengembangan sistem, di antaranya sebagai berikut:

A. Kriptografi

Kriptografi merupakan salah satu teknik dari beberapa teknik keamanan data yang sering digunakan untuk mengamankan data, seperti halnya menyandikan pesan asli (*plaintext*) ke dalam bentuk pesan rahasia (*ciphertext*). Proses pengaman ini melibatkan algoritma dan kunci. Kunci yang telah dienkripsi dapat dengan mudah dideskripsi kembali, yaitu dari ciphertext menjadi plaintext. Oleh karena itu diperlukan algoritma kriptografi yang kuat. Namun teknik ini masih menimbulkan kecurigaan pada orang lain yang melihat pesan tersebut. Menurut Munir Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Keamanan pesan diperoleh dengan menyandikannya menjadi pesan yang tidak mempunyai makna. Pesan yang dirahasiakan dinamakan *plainteks*, sedangkan pesan hasil penyandian disebut *cipherteks*. Proses penyandian plainteks menjadi *cipherteks* disebut enkripsi dan proses membalikkan *cipherteks* menjadi plainteks asalnya disebut dekripsi [16].

B. *Algoritma Advanced Encryption Standard* (AES)

AES merupakan algoritma enkripsi simetris untuk mengubah teks asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) menggunakan kunci enkripsi. AES adalah standar yang banyak digunakan dalam berbagai aplikasi, termasuk perlindungan data komunikasi dan penyimpanan data, karena kemampuannya yang kuat dalam menjaga keamanan data. Beberapa panjang kunci AES yaitu 128-bit, 192-bit, dan 256-bit.

Algoritma AES beroperasi pada tingkat byte, sehingga dapat dijelaskan dan diimplementasikan dengan mudah. *Key* dapat diperluas menjadi serangkaian sub-kunci individu, yang disebut sebagai kunci putaran yang digunakan pada setiap putaran operasi. Proses ekspansi kunci adalah langkah di mana kunci enkripsi diperluas untuk menghasilkan sepuluh *RoundKey* dalam proses enkripsi dan dekripsi. Kemudian, dalam proses enkripsi AES, terdapat empat jenis transformasi byte yang terlibat, yakni *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* [18].

C. Steganografi

Kata steganografi berasal dari bahasa yunani, *steganos* yang artinya tersembunyi dan *graphien* yang artinya tulisan yang dapat diterjemahkan menjadi tulisan yang tersembunyi. Menurut Munir bahwa Steganografi didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia. Media yang digunakan umumnya merupakan suatu media yang berbedadengan media pembawa informasi rahasia, disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas [19].

D. Spread Spectrum

Spread spectrum adalah metode transmisi yang memanfaatkan *pseudo-noise*, yang tidak terkait dengan data informasi, sebagai pengendali bentuk gelombang untuk mengalirkan energi sinyal melalui jalur komunikasi yang memiliki lebar pita yang lebih luas daripada sinyal komunikasi itu sendiri. Teknik ini akan memperlakukan gambar penutup (*cover image*) sebagai noise atau pseudo-noise yang disisipkan ke dalam gambar penutup itu sendiri.

Dalam metode *Spread Spectrum*, penyisipan pesan melibatkan penggunaan kunci untuk mengenkripsi pesan. Sebelum pesan disisipkan ke dalam *cover-image*, area tempat pesan akan disisipkan harus ditentukan terlebih dahulu. Setelah wilayah penyisipan ditetapkan, proses spreading dilakukan dengan menggunakan faktor pengali skalar yang telah ditentukan[20].

E. MSE dan PSNR

MSE (*Mean Square Error*) merupakan metrik yang digunakan untuk mengukur rata-rata kuadrat perbedaan antara nilai piksel pada citra asli dan citra hasil modifikasi. MSE digunakan untuk mengevaluasi tingkat distorsi pada citra setelah proses modifikasi.

Rumus MSE :

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2\,(m,n)]2}{M \times N}$$

Gambar 1. Rumus MSE

Keterangan :

- I (i,j) : Nilai intensitas piksel pada citra asli.
- K(i,j) : Nilai intensitas piksel pada citra hasil modifikasi.

- M,N : Dimensi citra (lebar dan tinggi)

Semakin kecil nilai MSE, semakin rendah Tingkat distorsi yang terjadi pada citra hasil modifikasi

PSNR (*Peak Signal-to-Noise Ratio*) merupakan metrik yang digunakan untuk mengukur kualitas citra hasil modifikasi dengan membandingkan nilai intensitas maksimum piksel dengan tingkat noise (distorsi) yang dihasilkan.

Rumus PSNR :

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

Gambar 2. Rumus PSNR

Keterangan :

- R^2 : Nilai maksimum intensitas piksel (untuk citra 8-bit, nilainya adalah 255)
- MSE : Hasil perhitungan *Mean Square Error*

Nilai PSNR yang lebih tinggi menunjukkan kualitas citra hasil modifikasi yang lebih baik, dengan distorsi minimal.

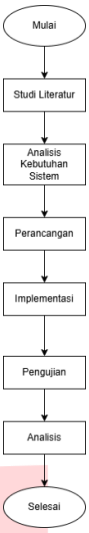
Secara umum :

- PSNR ≥ 30 dB : Kualitas dianggap baik
- PSNR diantara 20-30 dB : Kualitas masih dapat diterima
- PSNR < 20 dB : Kualitas dianggap buruk

Metode MSE dan PSNR digunakan untuk mengukur tingkat distorsi pada gambar setelah dilakukan proses penyisipan pesan terenkripsi menggunakan teknik Spread Spectrum. Nilai MSE pada gambar stego berada pada kisaran yang rendah, menandakan bahwa perubahan yang terjadi pada gambar sangat kecil. Selain itu, nilai PSNR yang diperoleh berada pada kisaran yang tinggi, yang mengindikasikan bahwa kualitas visual gambar stego masih menyerupai gambar asli, sehingga sulit dibedakan secara visual. Dengan demikian, metode *Spread Spectrum* yang digunakan untuk menyisipkan pesan dapat dianggap efektif dalam menjaga kualitas visual gambar dan meminimalkan dampak distorsi yang mungkin terjadi [21].

III. METODE

Pada penelitian ini, metode yang digunakan untuk pengamanan data teks melibatkan dua teknik utama yaitu Kriptografi AES (*Advanced Encryption Standard*) dan Steganografi *Spread Spectrum*. Berikut adalah langkah-langkah yang diterapkan dalam penelitian ini.



Gambar 3. Diagram Alir

A. Perumusan Masalah dan Studi Literatur

Pada tahap perumusan masalah ini merupakan tahap menentukan topik permasalahan yang akan dijadikan sebagai objek penelitian. Permasalahan yang diangkat penulis merupakan hal yang ingin diketahui seperti penerapan motode yang digunakan serta keefektifan dari pnerapan metode tersebut. Dalam melakukan penelitian, dibutuhkan referensi sebagai dasar untuk melakukan sebuah penelitian. Referensi yang digunakan dalam penelitian mengacu pada jurnal terdahulu yang berkaitan dengan penelitian yangakan dilakukan. Selain menggunaka jurnal, referensi penelitian juga dapat mengacu kepada buku untuk memahami lebih dalam metode yang diterapkan.

B. Tahap Analisis Kebutuhan Sistem

Bagian ini menjelaskan kebutuhan yang diperlukan untuk membangun sistem pengamanan data teks menggunakan kombinasi algoritma *Advanced Encryption Standard* (AES) dan metode steganografi gambar Spread Spectrum. Analisis kebutuhan ini mencakup kebutuhan perangkat keras, perangkat lunak, dan bahan yang digunakan, serta persyaratan teknis lainnya.

C. Tahap Perancangan

Perancangan sistem merupakan proses penggambaran dan pembuatan alur kerja sistem, serta gambaran-gambaran dari bentuk sistem memasuki tahap implementasi. Pada perancangan aplikasi merupakan proses pesan yang telah di enkripsi dengan AES dan disisipkan pada gambar.

D. Tahap Implementasi

Tahap implementasi dilakukan untuk merealisasikan rancangan sistem pengamanan data teks menggunakan algoritma *Advanced Encryption Standard* (AES) dan metode steganografi gambar *Spread Spectrum*. Proses dimulai dengan membangun antarmuka sistem yang ramah pengguna. Antarmuka ini dirancang agar pengguna dapat dengan mudah memasukkan data teks (*plaintext*) yang ingin diamankan dan memilih file gambar berformat PNG sebagai media penyisipan pesan. Setelah plaintext dimasukkan, sistem akan mengenkripsi data menggunakan algoritma AES. Proses enkripsi dimulai dengan padding data teks menggunakan aturan PKCS#7 jika panjang plaintext tidak sesuai dengan blok 16 *byte*. Kemudian, plaintext dan kunci enkripsi dikonversi menjadi matriks 4x4 untuk kebutuhan algoritma AES. Proses enkripsi dilanjutkan

dengan langkah-langkah seperti XOR plaintext dengan initial *round key* (*AddRoundKey*), *SubBytes*, *ShiftRows*, dan *MixColumns*, yang diulang hingga mencapai round ke-10. Hasil akhirnya berupa *ciphertext* yang aman dan sulit dipecahkan.

Selanjutnya, *ciphertext* yang dihasilkan dari proses enkripsi disisipkan ke dalam gambar menggunakan metode Spread Spectrum. Proses ini melibatkan *encoding ciphertext* menjadi bit-bit data, yang kemudian disisipkan secara acak ke dalam piksel gambar. Teknik *Spread Spectrum* memungkinkan penyisipan data secara tersembunyi dengan cara menyebarkan informasi ke dalam frekuensi gambar yang lebih luas, sehingga lebih sulit untuk dideteksi oleh pihak yang tidak berwenang. Dengan demikian, metode ini meningkatkan keamanan tidak hanya melalui enkripsi tetapi juga dengan menyembunyikan keberadaan data. Hasil dari proses ini adalah gambar baru (*stego-image*) yang telah berisi pesan terenkripsi, namun tetap menjaga kualitas visual gambar sehingga sulit dideteksi adanya perubahan. Sistem juga dilengkapi fitur opsional untuk mengekstraksi pesan dari gambar yang telah dimodifikasi. Proses ekstraksi melibatkan pembacaan *ciphertext* dari gambar, yang kemudian didekripsi menggunakan algoritma AES dengan kunci yang sesuai, sehingga plaintext asli dapat diperoleh kembali.

E. Tahap Pengujian

Tahap pengujian adalah tahap untuk memastikan seluruh kebutuhan telah diimplementasi bekerja dengan semestinya serta mengidentifikasi kekurangan dari sistem. Pada tahap ini terdapat beberapa hal yang akan dilakukan dalam pengujian yaitu :

a. Pengujian Enkripsi dan Deskripsi

Pengujian ini dilakukan untuk membuktikan apakah proses enkripsi pesan rahasia dapat diubah kedalam bentuk yang tidak dapat dimengerti oleh pihak ketiga. Dan sebbaliknya pada saat melakukan deskripsi, apakah pesan yang tidak dapat dimengerti tersebut dapat dikembalikan kedalam bentuk yang dapat dimengerti sesuai pesan aslinya tanpa mengurangi, menambahkan, dan memodifikasi isinya.

b. Pengujian kunci

Dalam pengujian kunci ini, yang digunakan untuk mengukur tingkat keamanan kunci yang digunakan. Alat ini menyediakan tiga metode pengecekan kunci, mencakup rentang dari kunci yang lemah hingga yang kuat, dan kunci yang digunakan adalah kunci dan pesan yang telah melalui proses enkripsi dan menyisipkan pesan ke dalam gambar pada program.

c. Pengujian File Algorima AES.

Tahap ini bertujuan untuk memastikan bahwa implementasi algoritma *Advanced Encryption Standard* (AES) 128-bit yang telah dirancang dapat berfungsi dengan baik dalam proses enkripsi dan dekripsi data. Pengujian dilakukan dengan menggunakan perangkat lunak yang dirancang secara khusus, tanpa melibatkan perangkat eksternal seperti OpenSSL, untuk menjaga keutuhan sistem dan memastikan hasil sesuai dengan tujuan penelitian. Proses pengujian diawali dengan mengenkripsi data teks menggunakan kunci enkripsi yang telah ditentukan. Hasil dari proses enkripsi berupa *ciphertext* diuji untuk memastikan bahwa data yang telah dienkripsi tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang. Selanjutnya, *ciphertext* yang dihasilkan diuji kembali melalui proses dekripsi untuk memastikan bahwa data dapat dikembalikan ke bentuk asli (*plaintext*) tanpa kehilangan informasi. Hasil pengujian menunjukkan bahwa algoritma AES-128 bekerja secara optimal dalam menjaga kerahasiaan data. Proses enkripsi menghasilkan *ciphertext* yang benar-benar acak dan sulit untuk dikenali. Proses dekripsi juga berhasil mengembalikan *ciphertext* tersebut menjadi *plaintext* dengan akurasi yang sempurna, tanpa adanya perubahan atau kerusakan data. Dengan demikian, pengujian ini membuktikan bahwa algoritma AES-128 yang digunakan dalam penelitian ini memiliki tingkat keamanan yang tinggi dan mampu menjaga integritas data selama proses pengamanan.

d. Pengujian File Algorima AES.

Langkah berikutnya adalah melakukan pengujian menggunakan Metode *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) untuk mengevaluasi kualitas citra sebelum dan setelah pesan disisipkan. Pengujian MSE dan PSNR dilakukan dengan memanfaatkan perangkat lunak *Visual Code Studio* dengan menggunakan rumus MSE dan PSNR.

F. Tahap Analisis

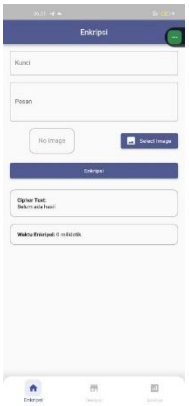
Tahap analisis dilakukan peneliti untuk menganalisis penerapan kriptografi dalam penyisipan pesan pada citra gambar dengan menggunakan kriptografi algoritma AES dan metode steganografi *Spread Spectrum*. Hal ini dilakukan untuk mendapatkan tingkat keamanan yang lebih tinggi guna melndungi pesan rahasia tetap aman. Dalam penerapan ini, pesan rahasia yang dienkripsi berupa pesan teks yang dibuat secara manual atau file berformat. sedangkan citra yang digunakan sebagai wadah penyisipan pesan menggunakan format file (*.png). proses ekstraksi berkas dengan cara memasukkan *stego-image* yang dihasilkan dari proses penyisipan guna mendapatkan ciphertext dan selanjutnya ciphertext dideskripsi agar mendapatkan pesan rahasia atau plaintext.

IV. HASIL DAN PEMBAHASAN

Bagian ini menghasilkan informasi dari langkah-langkah enkripsi, deskripsi, pengujian kunci dan pengujian gambar dan pengujian gambar yang telah disisipkan pesan dengan ciphertext yang diperoleh.

1. Proses Enkripsi

Hasil enkripsi pesan menggunakan AES pada gambar dibawah, dengan memasukkan sebuah kunci untuk mendapatkan hasil dari ciphertext, kemudian memasukkan pesan yang akan disisipkan kedalam gambar dengan format *.png*.



Gambar 4. Input Enkripsi

Setelah memasukkan kunci, maka ciphertext telah didapat dengan huruf acak yang tidak akan mudah di retas oleh pihak ketiga. Kemudian pesan yang telah dimasukkan juga telah disisipkan kedalam gambar yang dipilih.

Gambar 5. Hasil Enkripsi

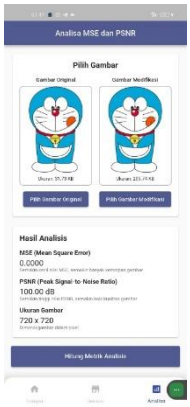
2. Proses Deskripsi

Hasil deskripsi adalah langkah dimana file gambar yang telah memiliki pesan tersembunyi dapat kembali diakses, dan plainteks akan kembali terbuka. Dan kita dapat melihat hasil deskripsi ini pada gambar dibawah ini.

Gambar 6. Hasil Deskripsi

3. Pengujian MSE dan PSNR

Langkah berikutnya adalah melakukan pengujian menggunakan *Metode Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) untuk mengevaluasi kualitas citra sebelum dan setelah pesan disisipkan. Pengujian MSE dan PSNR dilakukan dengan memanfaatkan perangkat lunak *VSCode* dengan menggunakan rumus MSE dan PSNR, dengan menjalankan pengujian pada berkas berformat .png



Gambar 7. Hasil Pengujian MSE dan PSNR

V. KESIMPULAN

Penelitian ini telah berhasil mengimplementasikan algoritma Advanced Encryption Standard (AES) dan metode steganografi Spread Spectrum untuk mengamankan data teks dalam media gambar. Proses enkripsi menggunakan algoritma AES yang melibatkan tahapan AddRoundKey, SubBytes, ShiftRows, dan MixColumns terbukti efektif dalam mengacak data sehingga sulit dikenali oleh pihak yang tidak berwenang. Selain itu, metode Spread Spectrum yang digunakan untuk menyisipkan pesan ke dalam gambar juga memberikan hasil yang baik, dengan perubahan kualitas gambar yang minim. Hasil pengujian menunjukkan bahwa tingkat perubahan kualitas gambar (MSE dan PSNR) masih berada dalam batas toleransi, sehingga gambar stego tetap terlihat alami tanpa terdeteksi adanya pesan tersembunyi. Sistem yang dirancang mampu mengenkripsi, menyisipkan, dan mengekstrak data teks dengan efisien. Ukuran gambar stego hanya mengalami perubahan minimal, yang tidak mengganggu fungsionalitas media gambar sebagai penampung informasi. Penggunaan algoritma AES-128 dengan kunci enkripsi yang kuat juga memberikan perlindungan tambahan terhadap serangan brute force. Pengujian keamanan menunjukkan bahwa sistem ini mampu menjaga kerahasiaan pesan dan mempersulit pihak yang tidak berwenang untuk mengakses informasi. Metode yang diterapkan dalam penelitian ini memberikan kontribusi signifikan dalam upaya meningkatkan keamanan data di era digital. Kombinasi antara kriptografi dan steganografi memastikan bahwa pesan tidak hanya terenkripsi secara logis, tetapi juga tersembunyi secara fisik dalam media gambar. Hal ini menunjukkan bahwa pendekatan yang digunakan sangat cocok untuk kebutuhan perlindungan data rahasia dalam berbagai aplikasi modern.

REFERENSI

[1] Ashadul, A. A. (2022). Aplikasi Steganografi Berbasis Android Menggunakan End of File dengan Enkripsi Rivest Code 4 Android-Based Steganography Application Using End of File with Rivest Code 4 Encryption. Jurnal KRESNA, Vol. 2, No. 2.

[2] Azhari, M., Perwitosari, J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, Vol. 2, No. 1, Hal. 2809–476.

[3] Davy Wiranata, A., & Aldisa, R. T. (2021). Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA. Jurnal Teknologi Informasi Dan Komunikasi), Vol. 5, No. 3.

[4] Diny Hermawati, F., & Tahir, M. (2023). Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada

Sistem AES (Advance Encryption Standard). In Jaya Abadi Amroin, Vol. 2, No 2.

[5] Fadhlurrohman, N. A. (2024). Penerapan Kriptografi Dengan Algoritma AES-128 Untuk Pengamanan Dokumen Digital Pada BPJS Kesehatan. Prosiding SENAFTI, Vol. 3, No 2.

[6] Frans Husein, Q., Furqan, M., & Ramadhan Nasution, Y. (2022). An Implementation Of Encryption And Decryption For Securing Document Data Using A Combination Advanced Encryption Standard And Rivest Code-4 Methods. Computer and Communication, Vol. 10, No. 5. http://infor.seaninstitute.org/index.php/infokum/index.

[7] Gunawan, I. (2023). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. Jurnal Media Informatika, Vol. 4, No 2.

[8] Herri Setiawan, Bedy Briliant Wijaya, & Dewi Sartika. (2023). Metode Spread Spectrum untuk Penyisipan Pesan pada Citra Digital. Bulletin of Computer Science Research, Vol. 4, No. 1, Hal. 101–111. https://doi.org/10.47065/bulletincsr.v4i1.310.

[9] Humayrah, R., Elhanafi, A. M., & Batubara, M. T. (2022). Analisa Histogram dan PSNR Pada Citra True Color Dalam Pengamanan Teks Menggunakan Spread Spectrum dan LSB Histogram and PSNR Analysis on True Color Image in Text Security Using Spread Spectrum and LSB. Jurnal Ilmu Komputer dan Sistem Informasi, Vol. 2, No 1. https://jurnal.unity-academy.sch.id/index.php/jirsi/index188.

[10] Siaulhak, S., & Kasma, S. (2023). Siaulhak, Safwan Kasma Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory. Journal of Informatics and Computer Engineering, Vol. 01, No 02.

[11] Kafa, N. A., Virgian, D., & Sakti, S. Y. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES) 256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. Jurnal TICOM: Technology of Information and Communication, Vol. 12, No. 2.

[12] Martawireja, A. R. H., Ridwan, R., Hafidzin, A. P., & Taufik, M. (2021). Proteksi Keamanan Data pada Quick Response (QR) Code. Jurnal Teknologi Dan Rekayasa Manufaktur, Vol. 3, No. 2, Hal. 99–110.

[13] Miftahul Amri, M., Waeno, M., & Zain Musa, M. (2023). LSB Steganography to Embed Creator's Watermark in Batik Digital Arts. Engineering Science Letter, Vol. 2, No. 1, Hal. 27–32. https://doi.org/10.56741/esl.v2i01.301.

[14] Multidisiplin Saintek, J., & Wanandi, R. (2024). Implementasi Sistem Steganografi Citra Dengan Metode Substitusi (Least Significant Bit). Vol. 2, No. 11, Hal. 10–20. https://ejournal.warunayama.org/kohesi.

[15] Iskandar, D. M., Nadip, M. Z., Dinilhaq, N., & Purnama, A. (2024). Penerapan Kriptografi AES Pada Fres-Caesas: Perlindungan Pesan Teks Dan Fail Dokumen. Journal of Information Technology and Computer Science, Vol. 7, No. 3.

[16] Pratama, Y. B., & Fachri, F. (2025). Analisis Keamanan Steganografi Pada Gambar Yang Diunggah Ke Media Sosial Menggunakan Least Significant Bit (LSB). Jurnal Mahasiswa Teknik Informatika, Vol. 9, No. 1.

[17] Tarigan, A. P. R., Ramadhan, P. S., & Ibnutama, K. (2023). Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard). Jurnal Cyber Tech STMIK Triguna Dharma, Vol. 5, No. 1.

[18] Romli, S. F., Hadiana, A. I., & Umbara, F. R. (2023). Penerapan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Spread Spectrum Untuk Mengamankan Pesan Dalam Gambar. Journal of Informatics and Communications Technology, Vol. 5, No. 2.

[19] Alya, A. N., Hamzah, I. W., & Ruriawan, M. F. (2022). Simulasi Dan Analisis Performansi Teknik Rivest Shamir Adleman (RSA) Pada Steganografi Least Significant Bit (LSB). E-Proceeding of Engineering, Vol. 8, No.6.

[20] Hidayatulloh, N. W., Tahir, M., Amalia, H., Basyar, N. A., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encrytion Standard (AES) Sebagai Algoritma Kriptografi Dalam Mengamankan Data. Digital Transformation Technology, Vol. 3, No. 1. https://doi.org/10.47709/digitech.v3i1.2293.

[21] Panjaitan, A. W., Zufria, I., & Nasution, Y. R. (2022). Implementation of Data Encryption Standard (DES) Algorithm for Data Security on PDF Documents. Jurnal Sains, Matematika, dan Terapan, Vol. 6, No. 2, Hal. 231–236.s