ANALISIS STEGANOGRAFIS PADA GAMBAR TERENKRIPSI MENGGUNAKAN RSA DAN DISCRETE WAVELET TRANSFORM

1st Ajeng Azzahra Noviqa Ramadhan
Telkom University Purwokerto
Purwokerto, Jawa Tengah
ajengazzahra@student.telkomuniversity.ac.id

2st Muhammad Fajar Shidiq
Telkom University Purwokerto
Purwokerto, Jawa Tengah
mfsidiq@telkomuniversity.ac.id

***Abstrak* — Keamanan data digital semakin krusial, terutama dalam transmisi informasi yang rentan terhadap akses ilegal. Penelitian ini menggabungkan kriptografi dan steganografi untuk meningkatkan perlindungan data. RSA digunakan dalam distribusi kunci, sedangkan AES berfungsi sebagai algoritma enkripsi utama. Pesan yang telah dienkripsi kemudian disisipkan ke dalam media digital menggunakan *Discrete Wavelet Transform* (DWT) untuk menyembunyikan informasi tanpa mengurangi kualitas media.**

Evaluasi dilakukan menggunakan *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE) guna mengukur kualitas media serta menguji ketahanan metode terhadap serangan. Hasil penelitian menunjukkan bahwa kombinasi kriptografi RSA-AES dan steganografi DWT mampu meningkatkan keamanan data serta mengurangi risiko akses tidak sah terhadap informasi sensitif.

***Kata kunci*— Keamanan data, Kriptografi, Steganografi, RSA, AES, DWT.**

I. PENDAHULUAN

Internet adalah lingkungan yang sangat tidak aman karena merupakan media komunikasi informasi yang tersimpan berupa gambar, suara, video, teks atau pesan lain. Kemajuan teknologi informasi, terutama di bidang komunikasi, semakin pesat. Seiring dengan berkembangnya media sosial, keamanan informasi dan privasi menjadi semakin krusial. Oleh karena itu, perlindungan data dalam transmisi internet perlu diperkuat agar tidak dapat diakses oleh pihak yang tidak berwenang [1].

Upaya yang di lakukan untuk meningkatkan keamanan data salah satunya dengan menerapkan teknik kriptografi. Kriptografi adalah ilmu yang melindungi data atau pesan selama pengiriman agar terhindar dari akses pihak ketiga. Pesan dalam bentuk teks dapat diamankan dengan enkripsi, mengubahnya menjadi karakter acak (ciphertext), dan hanya dapat dikembalikan ke bentuk aslinya melalui dekripsi oleh pemilik kunci [2].

Kriptografi ini bertujuan untuk menjaga kerahasiaan data yang di kirim melalui suatu media, sehingga tidak dapat di akses atau di curi oleh pihak yang tidak berwenang. Beragam metode kriptografi digunakan untuk mengamankan data dengan tingkat keamanan berbeda. Setiap metode memiliki keunggulan dan kelemahan, sehingga tantangan utamanya adalah memilih algoritma yang paling sesuai [3].

Berbagai Teknik telah di terapkan untuk melindungi data penting salah satunya adalah steganografi. Steganografi adalah metode menyembunyikan pesan dalam media lain agar tidak terdeteksi oleh pihak yang tidak berwenang. Berbeda dengan kriptografi yang mengenkripsi data, steganografi menyisipkan informasi ke dalam gambar, teks, audio, atau video tanpa menimbulkan kecurigaan [4]. Steganografi bertujuan untuk menyembunyikan data rahasia agar sulit terdeteksi serta melindungi hak cipta suatu produk. Data yang telah dienkripsi (ciphertext) disisipkan sedemikian rupa sehingga tidak disadari oleh pihak yang tidak berwenang [5].

Sementara itu dalam steganografi pada salah satu metode yang digunakan adalah *Discrete Wavelet Transform* (DWT) yang berfungsi membagi informasi suatu sinyal menjadi bagian pendekatan yang detail. Beberapa penelitian telah menggabungkan kriptografi dan steganografi untuk meningkatkan keamanan pesan, sehingga membuat pembajakan data lebih sulit karena selain menemukan pesan tersembunyi, juga diperlukan proses dekripsi. Salah satu studi meneliti kombinasi kriptografi dan steganografi berbasis *Discrete Wavelet Transform* (DWT) Haar, dengan citra sebagai media penyimpanan dan teks sebagai pesan rahasia. Metode DWT dipilih karena penelitian sebelumnya menunjukkan bahwa teknik ini mampu menghasilkan nilai *Peak Signal to Noise Ratio* (PSNR) lebih tinggi dibandingkan metode lain. Oleh karena itu, penelitian tersebut mengusulkan kombinasi kriptografi dan steganografi berbasis DWT pada audio, di mana teks berperan sebagai pesan rahasia dan audio sebagai media penyimpanan [6].

Penelitian ini mengembangkan metode untuk meningkatkan keamanan data dengan menggabungkan kriptografi dan steganografi dalam proses pengiriman informasi. Pesan rahasia dienkripsi menggunakan kriptografi, lalu disisipkan ke dalam media digital melalui steganografi berbasis *Discrete Wavelet Transform* (DWT), sehingga lebih sulit dideteksi atau diakses tanpa izin. Meskipun kombinasi

ini telah banyak diteliti, tantangan masih ada dalam meningkatkan ketahanan terhadap serangan, seperti analisis statistik dan brute force. Oleh karena itu, penelitian ini menerapkan steganografi pada gambar terenkripsi menggunakan RSA dan DWT untuk memperkuat perlindungan data, menjadikannya lebih aman dan sulit diretas.

II. KAJIAN TEORI

Bagian ini membahas teori-teori yang berkaitan dengan variabel penelitian sebagai landasan dalam pengembangan sistem, di antaranya sebagai berikut:

A. KeamananData

Keamanan data merupakan salah satu aspek yang sangat krusial dalam dunia teknologi informasi. Dengan pesatnya perkembangan teknologi digital, menjaga kerahasiaan, integritas, dan ketersediaan data menjadi semakin menantang. Data yang tidak terlindungi dengan baik rentan terhadap serangan siber seperti peretasan, pencurian informasi, dan penyebaran malware. Oleh karena itu, diperlukan metode perlindungan yang efektif untuk mengurangi risiko terhadap ancaman tersebut [7]. Menurut peneilitian (Kumar et al., 2019) terdapat beberapa faktor utama yang memengaruhi keamanan data, di antaranya adalah enkripsi, autentikasi, serta kontrol akses. Enkripsi adalah proses mengonversi data ke dalam format yang tidak dapat dibaca tanpa kunci dekripsi yang valid, sementara autentikasi memastikan bahwa pengguna yang mengakses data benar-benar memiliki izin. Sementara itu, kontrol akses berfungsi untuk membatasi pengguna berdasarkan hak dan izin yang telah ditetapkan dalam sistem keamanan [8].

B. Steganografi

Steganografi adalah teknik menyembunyikan pesan rahasia dalam media lain agar tidak terdeteksi oleh pihak yang tidak berwenang. Istilah ini berasal dari bahasa Yunani, "steganos" (tersembunyi) dan "graphos" (menulis). Dalam penerapannya, steganografi memerlukan media penampung seperti gambar, audio, video, atau teks untuk menyisipkan pesan, yang dapat berupa artikel, kode, atau informasi lainnya [9]. Steganografi adalah teknik menyembunyikan informasi agar tidak terdeteksi oleh pihak yang tidak berwenang. Dalam beberapa metode, data rahasia disisipkan langsung ke dalam media penampung (cover-object), menghasilkan stego-object yang tampak seperti media aslinya sehingga tidak menimbulkan kecurigaan saat dikirim [10].

Terdapat berbagai metodei steganografi yang telah dikembangkan untuk menyembunyikan pesan rahasia, antara lain:

Least Significant Bit (LSB), Transform Domain Techniques, Spread Spectrum Technique, Masking and Filteiring, Adaptive Steganography.

C. Kriptografi

Kriptografi beirasal dari kata Yunani crypto dan graphia. Crypto berarti secreit (rahasia) dan graphia berarti writing (tulisan). Kriptografi merupakan ilmu yang berfungsi untuk melindungi keamanan pesan saat dikirim dari satu lokasi ke lokasi lain. Secara sederhana, kriptografi menjaga kerahasiaan data dan informasi dengan cara menyamarkannya menjadi bentuk yang tidak dapat dipahami, sehingga hanya penerima yang bisa mengembalikannya ke bentuk aslinya [11].

Kriptografi mempunyai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua isu keamanan data dapat diatasi dengan kriptografi. Saat pesan dikirim, isinya dapat disadap oleh pihak ketiga yang tidak berhak mengetahuinya. Untuk melindungi pesan tersebut, isinya dapat diubah menjadi kode yang tidak dapat dipahami oleh orang lain. [12].

D. Citra Gambar

Citra merupakan representasi atau gambaran dari suatu objek yang dapat menyerupai atau menru bentuk aslinya. Teknik ini akan memperlakukan gambar penutup (cover image) sebagai noise atau pseudo-noise yang disisipkan ke dalam gambar penutup itu sendiri. Dalam sistem perekaman data, citra dapat muncul dalam berbagai bentuk, seperti foto (citra optik), sinyal video pada televisi (citra analog), dan format digital yang disimpan di media penyimpanan. Dalam komputasi, citra didefinisikan sebagai berkas digital yang merepresentasikan variasi warna dan intensitas cahaya dalam suatu gambar [13].

E. MSE dan PSNR

MSE (*Mean Square Error*) merupakan metrik umum untuk menilai kualitas gambar berbasis referensi penuh. Nilai mendekati nol menunjukkan hasil optimal, dengan MSE mengukur penyimpangan, varians, dan tingkat distorsi antara citra asli dan hasil rekonstruksi [14].

Rumus MSE :

$$MSE = \frac{1}{MN}\sum_{X}^{M} = 1 \sum_{Y}^{N} = 1 \, (S_{xy} - C_{xy})^2$$

Gambar 1. Rumus MSE

Keterangan :

- M : Jumlah elemen dalam dimensi horizontal (atau jumlah kolom data).
- N : Jumlah elemen dalam dimensi veirtikal (atau jumlah baris data).
- S_{xy} : Nilai sebenarnya (ground truth) pada posisi (x,y).
- C_{xy} : Nilai prediksi pada posisi (x,y).
- $(S_{xy} - C_{xy})^2$: Perbedaan kuadrat antara nilai sebenarnya dan nilai prediksi untuk elemen tertentu.

PSNR (*Peak Signal-to-Noise Ratio*) merupakan utuk mengukur kualitas gambar digital dengan membandingkan nilai maksimum sinyal dan tingkat noise. Perhitungan PSNR memerlukan nilai MSE, yang menunjukkan rata-rata error kuadrat antara citra asli dan hasil penyisipan, dengan hasil dinyatakan dalam decibel [15].

Rumus PSNR :

$$PSNR = 10 \, log \left(\frac{MAXi^2}{\sqrt{MSE}} \right)$$

Gambar 2. Rumus PSNR

Keterangan :

- PSNR : nilai PSNR (dalam Db)
- MAXi : nilai maksimum pikseil i
- MSE : nilai rata-rata error

F. Algoritma *Riveist Shamir Adleiman* (RSA)

Algoritma Rivest Shamir Adleman (RSA) merupakan algoritma kriptografi RSA dikategorikan sebagai algoritma asimeitris, di mana proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda. RSA menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Keamanannya bergantung pada sulitnya faktorisasi bilangan besar. Semakin besar bilangan prima, semakin tinggi keamanannya. RSA terdiri dari tiga tahap utama: pembuatan kunci, enkripsi, dan dekripsi untuk menjaga kerahasiaan serta integritas data [16].

G. Algoritma *Advanced Encryption Standard* (AES)

Advanceid Encryption Standard (AES) merupakan salah satu algoritma kriptografi simetris yang dapat digunakan untuk melakukan proses enkripsi dan deikripsi pada file maupun data. AES digunakan dalam sistem keamanan, termasuk enkripsi dan dekripsi e-mail, dengan metode penyandian berulang untuk meningkatkan keamanan. Kriptografi sendiri bertujuan menjaga kerahasiaan data dengan mengacak kunci enkripsi agar hanya dapat dibaca menggunakan kunci yang tepat [17].

H. Gambar Steganografi

Gambar steganografi ini berisi pesan rahasia (ciphertext) dalam file teks yang disisipkan ke dalam gambar berformat JPG atau PNG sebagai media penampung. Hasilnya berupa stego image dengan format sesuai gambar asal [18].

I. Jpeg

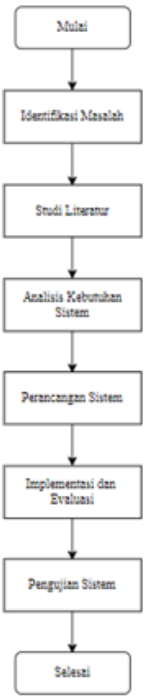
JPEG merupakan format gambar populer yang digunakan luas dalam berbagai aplikasi digital. Standar ini memungkinkan kompresi file tanpa mengurangi kualitas secara signifikan, sehingga efisien untuk penyimpanan dan transmisi gambar, terutama di internet. JPEG menjadi pilihan utama sejak era koneksi dial-up karena mampu mempercepat pengiriman data. Keunggulannya membuatnya standar industri di bidang fotografi, desain grafis, dan pengolahan citra [19].

J. Dart

Dart adalah bahasa pemrograman open-source yang dikembangkan oleh Google dan dirancang oleh Lars Bak serta Kasper Lund. Bahasa ini mendukung pengembangan aplikasi server, CLI, web, dan mobile (Android & iOS). Dart memiliki fitur top-level function serta sintaks mirip C-style dan berbasis OOP. Tidak seperti kebanyakan bahasa lain, Dart tidak memiliki array secara langsung, tetapi dapat mereplikasi strukturnya menggunakan generic dan tipe opsional untuk fleksibilitas dalam manipulasi data [20].

III. METODE

Pada penelitian ini mengamankan data teks dengan menggabungkan Kriptografi AES, RSA, dan Steganografi Discrete Wavelet Transform. Adapun langkah-langkah yang diterapkan dalam proses ini adalah sebagai berikut.



Gambar 3. Diagram Alir

A. Identifikasi Masalah

Pada tahap ini peneliti mengidentifikasi permasalahan yang muncul sehingga dapat meimbeirikan solusi yang bermanfaat untuk menyelesaikan permasalahan tersebut. Merancang latar belakang perlunya pemecahan suatu masalah, merumuskan masalah, mencari tujuan pemecahan masalah, dan mencapai manfaat berdasarkan tujuan penelitian yang dicapai.

B. Studi Literatur

Langkah selanjutnya adalah melakukan studi literatur. Pada tahap ini peneliti melakukan pengumpulan bahan referensi tentang pengamanan data, dari buku-buku, jurnal dan penelitian tugas akhir sebelumnya yang dapat membantu peneiliti untuk memecahkan masalah.

C. Analisa Kebutuhan Sistem

Pada Analisis kebutuhan pada sistem yang akan dirancang penulis yaitu analisis kebutuhan masukan (input), analisis keibutuhan proseis dan analisis keibutuhan hasil (output).

D. Perancangan Sistem

Pada tahap enkripsi, pengguna memilih metode (AES atau RSA), memasukkan pesan dan kunci, lalu menyimpan hasil enkripsi. Dekripsi dilakukan dengan memilih gambar terenkripsi dan memasukkan kunci untuk membaca pesan tersembunyi. Sementara itu, analisis membandingkan gambar asli dan terenkripsi menggunakan metrik seperti PSNR atau SSIM untuk mengevaluasi performa sistem. Pengguna dapat keluar melalui fitur logout. Alur ini dirancang untuk mengamankan data dan mengukur efisiensi sistem berbasis steganografi dan kriptografi.

E. Implementasi dan Evaluasi

Pada tahap implementasi melakukan langkah-langkah dari tahap sebelumnya yaitu perancangan sistem. Jika terdapat kesalahan atau kekurangan sistem dapat dilakukan perbaikan dengan melakukan evaluasi sistem.

F. Pengujian

Tahap pengujian sistem dilakukan untuk memastikan aplikasi memenuhi kebutuhan. Pengujian ini mencakup steganografi dan kriptografi guna meningkatkan keamanan pengiriman pesan. Pertama, pengujian kriptografi menggunakan algoritma RSA dan AES untuk mengenkripsi pesan menjadi chiperteks. Kedua, pengujian steganografi dilakukan dengan menyisipkan chiperteks ke dalam gambar menggunakan PSNR dan DWT. Setelah itu, ekstraksi dilakukan untuk memastikan hasil dekripsi sesuai dengan pesan asli. Analisis kualitas mencakup kecepatan, integrasi file, serta validasi data menggunakan PSNR dan DWT guna menjamin keakuratan pesan rahasia.

IV. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pengujian algoritma AES dan RSA dalam enkripsi, dekripsi, serta analisis kualitas data. Pengujian bertujuan mengevaluasi efektivitas dan efisiensi algoritma dalam menjaga keamanan data teks dan citra digital. Analisis dilakukan menggunakan MSE dan PSNR untuk mengukur perbedaan data sebelum dan sesudah enkripsi-dekripsi, serta waktu pemrosesan untuk menilai performa sistem. Pengujian mencakup berbagai skenario dengan variasi ukuran data guna memahami kinerja algoritma dalam kondisi berbeda. Hasilnya digunakan untuk mengidentifikasi kelebihan, keterbatasan, dan peluang pengembangan sistem lebih lanjut.

1. Proses Tampilan Login Pada Aplikasi

Proses login dimulai saat pengguna membuka aplikasi dan memasukkan username serta password. Sistem kemudian memvalidasi data dengan basis data. Jika sesuai, pengguna diarahkan ke halaman utama, namun jika salah, sistem meminta pengguna mencoba kembali.

Gambar 4. Halaman Tampilan Login

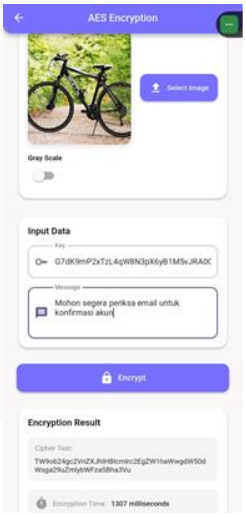
2. Proses Tampilan Home Pada Aplikasi

Setelah login atau tanpa autentikasi, halaman home dimuat dengan mengambil data dari basis data atau server. Antarmuka menampilkan menu utama seperti Enkripsi, Dekripsi, Analisis (AES & RSA), serta tombol Logout.

Gambar 5. Halaman Tampilan Home

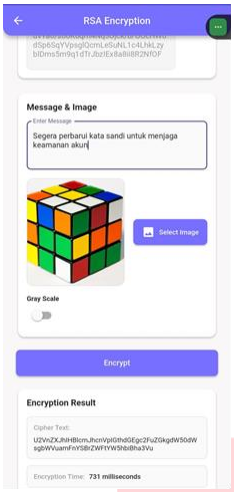
3. Proses Penyisipan Enkripsi AES dan RSA

Penelitian ini membuktikan keberhasilan enkripsi teks dengan algoritma AES, mengubah pesan menjadi ciphertext yang sulit dibaca tanpa kunci dekripsi. Dalam uji coba, pesan "*Mohon segera periksa email untuk konfirmasi akun*" dienkripsi dalam 1307 milidetik, menunjukkan efisiensi AES untuk skala kecil hingga menengah. Keamanan bergantung pada kunci yang digunakan, sehingga dekripsi tanpa kunci yang sesuai tidak mudah dilakukan. AES efektif dalam melindungi komunikasi dan data pribadi, meskipun efisiensinya dipengaruhi oleh panjang kunci, ukuran data, dan performa perangkat.



Gambar 6. Halaman Tampilan Enkripsi AES

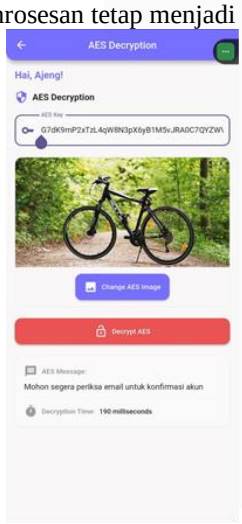
Setelah itu proses enkrupsi RSA Aplikasi ini menerapkan algoritma RSA untuk mengenkripsi teks, mengubah pesan "*Segera perbarui kata sandi untuk menjaga keamanan akun*" menjadi ciphertext menggunakan kriptografi kunci publik. Hasil enkripsi menghasilkan karakter acak tanpa makna langsung, meningkatkan keamanan data. Proses ini memakan waktu 731 milidetik, menunjukkan efisiensi RSA untuk skala kecil hingga menengah. RSA bekerja dengan pasangan kunci publik dan privat, di mana hanya penerima dengan kunci privat yang sesuai dapat mendekripsi pesan. Meskipun efektif untuk komunikasi digital, penggunaannya harus mempertimbangkan keseimbangan antara keamanan dan efisiensi pemrosesan.



Gambar 7. Halaman Tampilan Enkripsi RSA

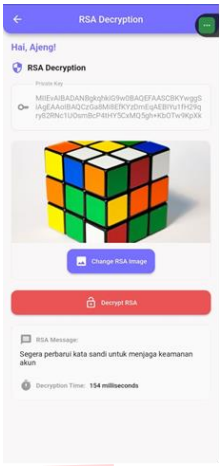
4. Proses Penyisipan Deskripsi AES dan RSA

Proses dekripsi menggunakan algoritma AES berhasil mengembalikan pesan terenkripsi menjadi teks asli: "*Mohon segera periksa email untuk konfirmasi akun*." Dengan waktu dekripsi 190 milidetik, AES terbukti efisien dalam memproses data terenkripsi. Keberhasilan ini menunjukkan bahwa hanya pengguna dengan kunci yang sesuai yang dapat mengakses informasi. Implementasi AES menegaskan efektivitas kriptografi simetris dalam perlindungan data dan keamanan digital. Namun, pada skala besar, keseimbangan antara keamanan dan efisiensi pemrosesan tetap menjadi faktor penting.



Gambar 8. Halaman Tampilan Desskripsi AES

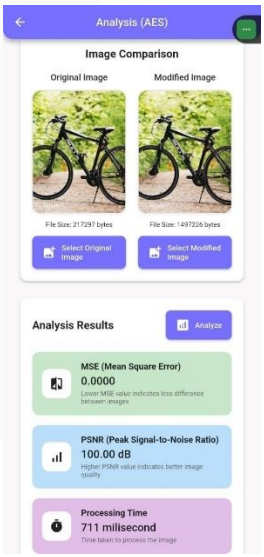
Setelah itu proses dekripsi dengan algoritma RSA berhasil mengembalikan pesan terenkripsi menjadi teks asli: "*Segera perbarui kata sandi untuk menjaga keamanan akun*," dalam 154 milidetik. RSA, sebagai algoritma kriptografi asimetris, menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Meskipun lebih kompleks dibandingkan AES, RSA tetap efektif untuk keamanan data, terutama dalam autentikasi dan perlindungan informasi sensitif. Namun, pada skala besar, efisiensi dan panjang kunci perlu diperhatikan untuk menjaga keseimbangan antara keamanan dan kinerja sistem.



Gambar 9. Halaman Tampilan Desskripsi RSA

5. Proses Analisis Hitungan *Peak Signal to Noise Ration* (PSNR) dan *Mean Squared Error* (MSE)

Analisis perbandingan citra asli dan terenkripsi dengan AES menunjukkan MSE sebesar 0.0000, menandakan tidak ada perbedaan piksel. Nilai PSNR mencapai 100.00 dB, menunjukkan kualitas dekripsi hampir identik dengan gambar asli. Proses ini berlangsung dalam 711 milidetik, membuktikan efisiensi AES dalam pengolahan citra digital. Hasil ini mengonfirmasi bahwa metode enkripsi dan dekripsi AES memiliki akurasi tinggi, sehingga cocok untuk sistem keamanan digital tanpa mengurangi kualitas visual.



Gambar 10. Halaman Tampilan Analisis AES Hitungan PSNR dan MSE

Setelah itu analisis kualitas citra dengan RSA menggunakan PSNR dan MSE menunjukkan MSE sebesar 0.0000, menandakan perbedaan antara gambar asli dan terenkripsi sangat kecil atau tidak terdeteksi. PSNR mencapai 100.00 dB, menunjukkan kemiripan tinggi dengan gambar asli. Proses ini berlangsung dalam 607 milidetik, membuktikan efisiensi metode yang digunakan. Hasil ini menegaskan efektivitas algoritma serta memberikan wawasan terkait penerapan PSNR dan MSE dalam analisis kualitas citra digital.

Gambar 11. Halaman Tampilan Analisis RSA Hitungan PSNR dan MSE

V. KESIMPULAN

Penelitian ini menyimpulkan bahwa kombinasi kriptografi dan steganografi meningkatkan keamanan data dalam transmisi informasi. AES efektif untuk enkripsi cepat, sementara RSA memastikan distribusi kunci yang aman. Teknik DWT dalam steganografi berhasil menyisipkan data tanpa menurunkan kualitas gambar, dibuktikan dengan MSE rendah (0.0000) dan PSNR tinggi (100.00 dB).

Uji coba menunjukkan bahwa waktu pemrosesan bervariasi sesuai ukuran data dan algoritma yang digunakan, dengan AES lebih cepat dari RSA. Kombinasi kedua algoritma ini memberikan keseimbangan antara efisiensi dan keamanan. Metode ini dapat diterapkan dalam perlindungan data komunikasi, keamanan digital, dan sistem autentikasi berbasis kriptografi. Penelitian lebih lanjut dapat mengoptimalkan enkripsi dan steganografi untuk meningkatkan efisiensi dan keandalan sistem.

REFERENSI

[1] M. Betty Yel and M. K. M Nasution, "*Keamanan Informasi Data Pribadi Pada Media Sosial,"* JIK), vol. 6, no. 1, 2022.

[2] F. Musadat and J. Nur, *"Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64,"* Jurnal Informatika, vol. 7, no. 2, 2018, [Onlinei]. Available: http://ejournal.unidayan.ac.id/index.php/JIU/issue/view/10

[3] M. R. Fahlev, D. Ridha, D. Putri, and R. Doni, *"Teknik Keamanan File Teks Menggunakan Kriptografi Dengan Algoritma One Time Pad Cipher,"* Jurnal Sains Komputer & Informatika (J-SAKTI, vol. 4, no. 2, pp. 588–597, 2020.

[4] A. Gustiawan, J. Wahyudi, and E. Suryana, *"Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Dfferencing,"* JUKI: Jurnal Komputer dan Infromatika, vol. 5, pp. 151–163, 2023.

[5] N. Nurmaesah, T. Lestari, and A. Retno Mariana, "*Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image*," *Technology Acceptance Model*, vol. 8, no. 1, pp. 13 – 17, 2017

[6] N. Laila and A. S. Rms, *"Implementation of LSB Steganography with Vigenere Cipher Encryption in Image, "Computer Science Informatics Journal*, vol. 1, no. 2, pp. 47-58, 2018.

[7] A. Kumar, R. Kumar, and V. K. Sharma, *"Data Security: A Review on Concept, Concerns and Methods,"* SSRN Electronic Journal, pp. 1376-1380, 2019, doi: 10.2139/ssm.3356494.

[8] J. Mul and S. Volume, *"Kata Kunci: Privasi Data, Keamanan Data, Solusi, E-Commerce,"* vol. 3, no. 9, 2024.

[9] J. Rekursif, H. Ardiansyah, B. Susilo, and A. Erlansari, *"Penerapan Metode DCT (Discrete Cosine Transform) pada Aplikasi Penyembunyian,"* Jurnal Rekursif vol. 5, no. 1, pp. 66-74, 2017.

[10] J. Pardosi, *"Penyembunyian Pesan Pada File Audio Menerapkan Metode Chineseremainder Theorem,"* Media Online), vol. 1, no. 6, pp. 326-334, 2021, [Online]. Available: https://djournals.com/resolusi

[11] I. A. R. Simbolon, I. O. Kirana, R. Dewi, and S. Solikhun, *"Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantara," Journal of Computer System and Informatics* (JoSYC), vol. 1, no.2, pp. 54-60, 2020.

[12] R. Maulana and R. M. Simanjorang, *"Implementasi Kriptografi Pengamanan Data Pribasi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4,"* Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI), vol. 4, no. 6, pp. 377-383, doi: 10.32672/jnki.v4i63533.

[13] U. Aplikasi, *"Analisa Kualitas Citra Pada Steganografi,"* Program, pp. 1-9,2012.

[14] R. Renaldy and J. Informatika, "1, 2, 3," vol.9, no. Sens 9, pp. 588-596, 2024.

[15] R. Fahmi, N. Imanudin, I. Kustiawan, and S. Elvyanti, *"Steganografi Citra Digital Menggunakan Pendekatan Least Significant Bit dan Discrete Cosine Transform,"* Seminar Nasional Teknik …, no. 207, pp. 1-5, 2023, [Online]. Available: https://snte.fortei.org/list/index.php/snte/article/view/48%0Ahttps://snte.fortei.org/list/index.php/snte/article/download/48/50

[16] S. Kasus, P. Presiden, and M. Stmik. *"Implementasi Kriptografi Dalam Pengamanan Database E-Votting Menggunakan Algoritma RSA Dan Base64 Berbasis Progresive Web Apps,"* e-Jurnal JUSITI (Jurnal Sistem Informasi dan Teknologi Informasi), vol. 10, no. 1, pp. 30-40, 2021, doi:10.36.774/jusiti.v10il.818.

[17] Fadlullah Fadlullah et al., *"Implementasi Algoritma AES pada Autentikasi Login Sistem Informasi,"* Jurnal Bintang Pendidikan Indonesia, vol. 1, no. 2, pp. 251-263,2023,doi:10.55606/jubpi.v1i2.1420.

[18] A. R. Hakim and W. M. Baihaqi. *" Komputa : Jurnal Ilmiah Komputer dan Informatika Tiket Pesawat Berbasis Web Komputa : Jurnal Ilmiah Komputer dan Informatika,"* vol. 12, no. 2, pp. 50-58,2023

[19] D. T. Elektro, "2.2 Par 2," vol. 10, no. 2, pp. 277-284,2021

[20] M. Muslim, R. P. Sari, and S. Rahmayuda, *"Implementasi Framework Flutter Pada Sistem Informasi Perpuastakaan Masjid,"* Coding Jurnal Komputer dan Aplikasi, vol. 10, no. 01, p. 46,2022, doi: 10.26418/coding.v10i01.52178.