

Data Security Optimization Using AES in Cipher Block Chaining (CBC) Mode with RSA Asymmetric Key Distribution

Deranda Bagas Pamungkas¹, Christy Atika Sari^{2*}, Chaerul Umam³

Informatics Engineering, Universitas Dian Nuswantoro

111202314906@mhs.dinus.ac.id¹, christy.atika.sari@dsn.dinus.ac.id³, chaerul@dsn.dinus.ac.id³

Article Info

Article history:

Received 2026-08-11

Revised 2026-09-11

Accepted 2026-10-15

Keywords:

Data security,
Advanced Encryption Standard,
Rivest-Shamir-Adleman,
Cipher Block Chaining,
PSNR,
Entropy.

ABSTRACT

Transmitting digital images over public networks makes them vulnerable to data manipulation. While the AES algorithm offers high encryption speeds, it is weak regarding symmetric key distribution; conversely, RSA is robust for key exchange but computationally too heavy for large-capacity image data. Therefore, this study proposes a hybrid cryptographic algorithm that integrates the scrambling speed of AES in Cipher Block Chaining (CBC) mode with the secure asymmetric key distribution of RSA. The system underwent comprehensive bidirectional evaluation (encryption and decryption) using Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Information Entropy, Histogram Analysis, Spatial Pixel Correlation, and Computational Time metrics on the standard USC-SIPI dataset. Test results demonstrate extreme visual degradation during the encryption phase, characterized by an MSE of 10,133 and a PSNR reduced to 8.07 dB. The CBC mode successfully eliminated statistical patterns, validated by an entropy value of 7.9998, a uniform distribution in the encrypted image histogram, and spatial pixel correlation values plummeting to near zero. During the decryption phase, the algorithm achieved 100% lossless image recovery (MSE of 0, PSNR of 100 dB, and preserved entropy). The proposed AES-RSA hybrid system proves to be robust against statistical analysis while ensuring precision in image recovery.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. PENDAHULUAN

Perkembangan teknologi informasi saat ini telah meningkatkan arus pertukaran data multimedia secara drastis melalui jaringan terbuka. Gambar atau citra digital menjadi salah satu jenis data yang paling sering dikirimkan pada berbagai sektor penting, mulai dari sistem pengawasan hingga bidang medis. Namun, pengiriman gambar melalui jaringan publik sangat rentan terhadap kejahatan siber berupa penyadapan dan manipulasi data [1]. Apabila kebocoran informasi ini menimpa data yang sangat rahasia, seperti rekam medis pasien, hal tersebut tentu dapat menyebabkan pelanggaran privasi yang sangat fatal [2]. Selain itu, sebuah citra digital umumnya memiliki ukuran data yang besar dan pola warna piksel yang saling berkaitan erat. Karakteristik alami ini membuat citra digital sangat sulit dilindungi menggunakan algoritma enkripsi teks biasa, sehingga lebih rentan terhadap eksploitasi serangan analisis statistik modern

[3]. Oleh karena itu, dibutuhkan sebuah sistem kriptografi khusus yang kuat untuk mengamankan data visual tersebut sebelum dikirimkan melalui jaringan komunikasi.

Dalam perkembangannya, pengamanan data multimedia menuntut algoritma kriptografi yang memiliki efisiensi komputasi tinggi akibat besarnya kapasitas dan tingginya korelasi piksel pada citra digital [4], [5]. Salah satu algoritma standar yang paling umum digunakan untuk menangani hal tersebut adalah Advanced Encryption Standard (AES) [4]. Meskipun AES terbukti sangat cepat dan tangguh dalam mengacak matriks piksel citra, algoritma ini memiliki kelemahan struktural pada aspek distribusi kunci karena menggunakan kunci simetris yang sama untuk proses enkripsi dan dekripsi [6]. Di sisi lain, algoritma asimetris seperti Rivest-Shamir-Adleman (RSA) dengan panjang kunci 2048-bit menawarkan keamanan distribusi kunci tingkat tinggi melalui mekanisme kunci publik dan privat. Namun, RSA melibatkan operasi matematika modular yang sangat berat,

sehingga membuatnya sangat lambat dan sangat tidak efisien jika dipaksa untuk mengenkripsi kapasitas data citra yang besar secara langsung [6]. Oleh karena itu, penerapan algoritma tunggal seringkali tidak memadai untuk mencapai keseimbangan antara kecepatan eksekusi dan keamanan pertukaran kunci pada jaringan publik.

Berbagai penelitian telah dilakukan untuk meningkatkan keandalan enkripsi pada citra standar internasional seperti Lena, Mandrill (Baboon), dan Peppers dengan resolusi 512x512. Sebagai contoh, penelitian pada literatur [7] mengembangkan sistem kriptografi hybrid dan mengevaluasinya menggunakan parameter Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Information Entropy, Analisis Histogram, dan Korelasi Piksel Spasial. Meskipun sistem tersebut mampu menghasilkan keacakan sandi yang baik, tingkat kerusakan struktural citra sandinya (MSE) masih tergolong rendah dan penelitian tersebut tidak memvalidasi kualitas pemulihan citranya pada tahap dekripsi. Pendekatan serupa juga dilakukan dalam penelitian [8] yang mengusulkan skema enkripsi citra ringan pada dataset standar, namun pengujiannya masih berfokus eksklusif pada tahap enkripsi saja. Lebih lanjut, penelitian terbaru [9] berhasil mencapai tingkat noise (PSNR) dan Entropy yang sangat kuat menggunakan dataset USC-SIPI. demikian, penelitian tersebut memiliki celah pengujian karena tidak menyertakan citra standar Lena, tidak menampilkan nilai ukur distorsi (MSE), serta tidak membuktikan efisiensi dekripsi secara matematis. Berdasarkan celah pada ketiga literatur tersebut, penelitian ini mengusulkan algoritma kriptografi hybrid AES-RSA. Algoritma ini memiliki kebaruan spesifik pada pembangkitan kunci sesi dinamis dan evaluasi dua arah. Secara teknis, sistem membangkitkan AES session key secara acak (dinamis) setiap kali proses enkripsi berjalan. Kunci sesi tersebut kemudian dienkripsi secara independen menggunakan algoritma RSA guna menjamin keamanan distribusinya. Pendekatan dinamis ini menghasilkan parameter kunci yang selalu unik pada setiap citra untuk menutup celah eksploitasi kunci statis. Selanjutnya, peneliti memvalidasi efektivitas algoritma melalui pengujian komprehensif guna mengatasi kelemahan pengujian pada literatur [7], [8], dan [9]. Pengujian tersebut mencakup pengukuran daya rusak visual (MSE dan PSNR), keacakan spasial (Entropy), serta pembuktian pemulihan citra tanpa cacat (lossless) pada seluruh dataset standar.

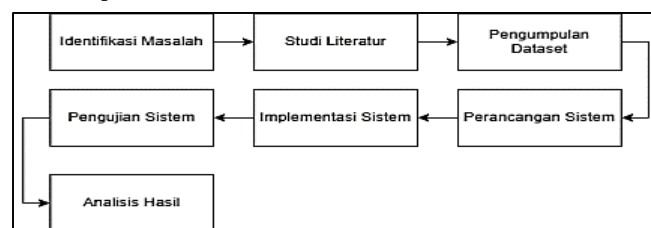
Secara teknis, peneliti merancang komponen enkripsi AES pada sistem ini menggunakan mode Cipher Block Chaining (CBC) untuk memperkuat pengacakan matriks citra, sementara algoritma RSA bertugas mengamankan distribusi kuncinya. Selanjutnya, peneliti mengevaluasi sistem menggunakan metrik standar internasional, yakni Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Information Entropy, Analisis Histogram, Korelasi Piksel Spasial, serta Waktu Komputasi. Pemilihan metrik evaluasi ini secara spesifik merujuk pada parameter ukur performa kunci pelindung citra digital yang disarankan oleh literatur

[10]. Evaluasi komprehensif tersebut bertujuan untuk membuktikan secara akademis bahwa pendekatan keamanan berlapis (hybrid) terbukti mampu memberikan tingkat ketahanan perlindungan data yang jauh lebih superior dibandingkan algoritma enkripsi tunggal konvensional yang rentan terhadap serangan siber [11], [12]. Terakhir, peneliti mengeksekusi seluruh tahapan pengujian ini secara konsisten menggunakan dataset citra standar dari basis data USC-SIPI, khususnya citra Lena, Mandrill, dan Peppers beresolusi 512x512 piksel.

Sebagai kontribusi praktis, penelitian ini mengimplementasikan algoritma *hybrid* AES-RSA ke dalam perangkat lunak berbasis antarmuka grafis (GUI) untuk memfasilitasi proses enkripsi dan dekripsi citra digital secara efisien. Aplikasi ini juga dirancang untuk menguji performa algoritma secara otomatis menggunakan parameter Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Information Entropy, Analisis Histogram, dan Korelasi Piksel Spasial. Implementasi ini diharapkan mampu memberikan solusi perlindungan data visual yang teruji secara nyata, aman, dan dapat diterapkan.

II. METODE

A. Tahapan Penelitian



Gambar 1 Tahapan Penelitian

Penelitian ini dilaksanakan melalui serangkaian tahapan yang disusun secara sistematis agar pengembangan sistem berjalan terarah, sebagaimana ditunjukkan pada blok diagram Gambar 1.

1. Identifikasi Masalah

Peneliti menganalisis tingkat kerentanan citra digital dan kelemahan algoritma tunggal pada tahap ini dalam menemukan solusi pengamanan berbasis sistem hybrid.

2. Studi Literatur

Peneliti mengkaji landasan teori algoritma AES, RSA, dan parameter evaluasi citra dari berbagai jurnal terdahulu sebagai dasar perancangan sistem.

3. Pengumpulan Dataset

Peneliti mengunduh tiga berkas citra digital berformat PNG (Pappers, Mandril, Lena) dari repositori publik Kaggle untuk digunakan sebagai data uji sistem.

4. Perancangan Sistem

Peneliti merancang arsitektur enkripsi-dekripsi hybrid AES-RSA beserta antarmuka pengguna (GUI) secara sistematis agar aplikasi berjalan sesuai tujuan penelitian.

5. Implementasi Sistem

Peneliti membangun aplikasi Hybrid Crypto Analyzer menggunakan bahasa pemrograman Python dan pustaka PyCryptodome pada tahap implementasi ini.

6. Pengujian Sistem

Peneliti menguji kinerja algoritma hybrid pada ketiga dataset citra untuk menghasilkan metrik perhitungan durasi komputasi, MSE, PSNR, Entropy, Analisis Histogram, dan Korelasi Pixel.

7. Analisis Hasil

Peneliti mengevaluasi seluruh data matematis hasil pengujian secara menyeluruh untuk menyimpulkan tingkat kualitas pemulihan visual dan keamanan statistik.

B. Pengumpulan Dataset

Data uji yang digunakan dalam eksperimen ini pada dasarnya bersumber dari basis data standar USC-SIPI (University of Southern California - Signal and Image Processing Institute), yang secara luas diakui sebagai tolak ukur (benchmark) utama berskala internasional dalam penelitian pengolahan citra dan kriptografi. Untuk keperluan penelitian ini, seluruh objek citra sekunder tersebut diunduh secara sah melalui repositori publik Kaggle [13]. Meskipun basis data USC-SIPI menyediakan ratusan dataset, penelitian ini berfokus mengekstraksi 3 (tiga) sampel gambar utama, yakni Lena, Mandrill (Baboon), dan Peppers.

TABEL I
DATASET CITRA YANG DIGUNAKAN

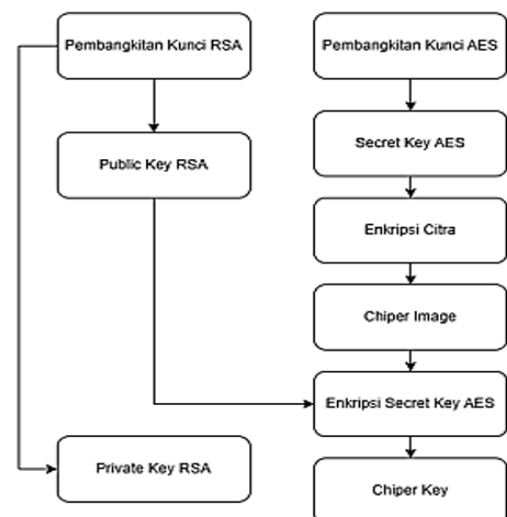
No	Nama Citra	Dimensi (Piksel)	Visualisasi Citra
1	Pepper.png	512 × 512	
2	Baboon.png	512 × 512	
3	Lena.png	512 × 512	

Seluruh dataset citra uji tersebut diekstraksi ke dalam format file Portable Network Graphics (PNG) dengan jenis citra berwarna (kedalaman 24-bit RGB) dan memiliki resolusi dimensi spasial yang seragam, yakni 512 × 512 piksel. Pemilihan ketiga gambar standar ini didasarkan pada variasi karakteristik visual dan kompleksitas tekstur yang sangat berbeda. Hal ini secara khusus bertujuan untuk menguji batas ketangguhan algoritma enkripsi pada berbagai

skenario; citra Mandrill mewakili kompleksitas tekstur frekuensi tinggi (sangat rumit), Peppers mewakili area warna yang halus, dan Lena merepresentasikan perpaduan fitur wajah serta kontras pencahayaan. Perbedaan tingkat kompleksitas warna dan tekstur ini dimanfaatkan untuk membuktikan bahwa algoritma hibrida AES-RSA mampu menghasilkan tingkat keacakan sandi yang konsisten tanpa terpengaruh oleh karakteristik piksel bawaan dari citra aslinya.

C. Perancangan Sistem

Penelitian ini merancang arsitektur pengamanan citra digital menggunakan pendekatan hybrid AES-128 dan RSA-2048 bit berbasis antarmuka grafis (GUI). AES dipilih karena keunggulannya mengacak matriks data secara cepat melalui transformasi matematis kompleks [14]. Secara spesifik, sistem mengimplementasikan AES mode Cipher Block Chaining (CBC). Mode ini dipilih karena memiliki efek perambatan (avalanche effect) yang kuat antarblok, sehingga ideal untuk memaksimalkan distorsi piksel citra uji. Peneliti menyadari mode CBC secara intrinsik tidak menyediakan authentication (seperti mode GCM), sehingga rentan terhadap manipulasi atau padding-related attacks di jaringan publik. Namun, karena sistem ini difokuskan sebagai instrumen analitik tertutup (Crypto Analyzer) untuk pengujian komparatif metrik visual secara lokal, mekanisme autentikasi tambahan tidak diintegrasikan. Pengamanan jalur distribusi kunci sepenuhnya diserahkan pada algoritma RSA [15]. Penambahan Message Authentication Code (MAC) menjadi rekomendasi pengembangan sistem untuk transmisi publik di masa mendatang. Rincian alur kerja sistem ditunjukkan pada Gambar 2 dan Gambar 3.

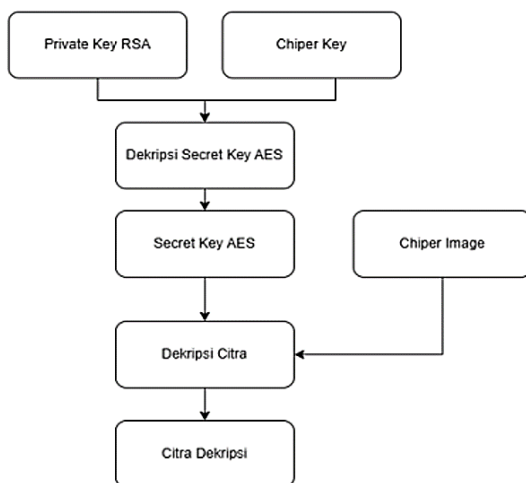


Gambar 2 Proses Enkripsi Citra

1. Perancangan Proses Enkripsi

Sistem enkripsi pada penelitian ini mengacak citra asli melalui perpaduan dua lapis algoritma kriptografi yang dioptimalkan [16]. Pada lapisan pertama, sistem

mengonversi citra menjadi format array byte dan mengenkripsinya menggunakan block cipher AES [14]. Operasi enkripsi ini berjalan pada mode Cipher Block Chaining (CBC) dengan panjang kunci 128-bit serta menggunakan Initialization Vector (IV) yang dibangkitkan secara acak [17]. Kombinasi mode CBC dan IV acak tersebut menjamin bahwa hasil cipher-image selalu bervariasi secara dinamis pada setiap eksekusi. Selain itu, serangkaian operasi matematis internal AES (SubBytes, ShiftRows, MixColumns, AddRoundKey) bertugas mendistorsi susunan matriks piksel secara maksimal. Pada lapisan kedua, algoritma RSA (public-key) mengenkripsi kunci rahasia AES tersebut secara asimetris demi menjamin keamanan distribusinya pada jaringan publik. Mengingat aplikasi ini dirancang secara spesifik sebagai instrumen pengujian analitik (analyzer), sistem tidak mempacketkan keluaran akhirnya (cipher-image, IV, dan AES key terenkripsi RSA) ke dalam satu berkas fisik (hybrid encrypted file). Sebagai gantinya, sistem mengalokasikan seluruh parameter dinamis tersebut secara aman di dalam memori internal sesi pengujian (session state) agar dapat langsung dievaluasi pada tahapan dekripsi selanjutnya.



Gambar 2 Proses Dekripsi Citra

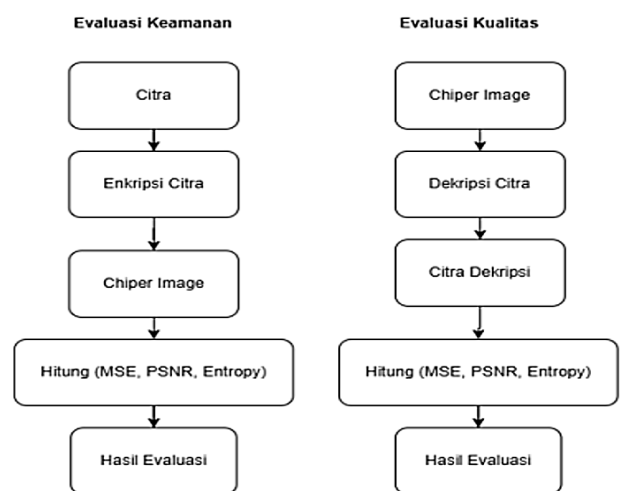
2. Perancangan Proses Dekripsi

Perancangan proses dekripsi merupakan skema pemulihan (recovery) secara utuh dari tahap enkripsi. Pada tahap ini, sistem terlebih dahulu memecahkan kunci rahasia AES yang masih dalam keadaan terkunci. Proses ini dieksekusi menggunakan algoritma asimetris RSA dengan cara memasukkan private key milik penerima data untuk mengekstraksi cipher key kembali menjadi kunci rahasia AES murni [15], serta memanggil kembali Initialization Vector (IV) secara langsung dari memori sesi pengujian [17]. Setelah secret key dan IV AES berhasil ditarik secara valid dari memori, aplikasi menjalankan operasi inversi (kebalikan) dari algoritma block cipher AES mode CBC [14], seperti InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey secara presisi ke

dalam matriks citra sandi. Transformasi balik ini secara matematis akan merekonstruksi susunan piksel yang teracak sehingga mengembalikan citra digital ke wujud aslinya tanpa degradasi data sedikit pun (100% lossless).

D. Skenario Pengujian

Peneliti menyusun skenario pengujian secara terstruktur untuk mengukur efektivitas dan kinerja dari sistem kriptografi hybrid AES-RSA secara keseluruhan. Peneliti mengevaluasi setiap tahapan proses menggunakan tiga parameter ukur utama sekaligus, yaitu evaluasi kualitas pemulihan visual (MSE dan PSNR) serta evaluasi tingkat keamanan statistik (Entropy). Rincian tahapan langkah demi langkah dari proses pengujian sistem ini digambarkan secara visual pada Gambar 2.4.



Gambar 3 Proses Evaluasi Parameter

Berdasarkan Gambar 4, peneliti melaksanakan skenario pengujian melalui tahapan terstruktur berikut:

1. Tahap (Evaluasi Keamanan)

Peneliti memproses citra uji asli menggunakan algoritma enkripsi. Sistem kemudian menghasilkan citra tersandi, yang mana tingkat keamanannya langsung diukur oleh peneliti menggunakan perhitungan parameter Entropy, MSE, dan PSNR serta Analisis Histogram dan Korelasi Piksel Spasial secara bersamaan untuk memvalidasi tingkat keacakan datanya.

2. Tahap (Evaluasi Kualitas Visual)

Peneliti membawa citra tersandi tersebut ke dalam proses dekripsi untuk memulihkannya kembali menjadi citra hasil dekripsi.

3. Validasi Akhir

Terakhir, peneliti secara langsung membandingkan citra hasil dekripsi tersebut dengan citra aslinya. Peneliti kembali menghitung nilai Entropy, MSE, dan PSNR untuk memvalidasi dan membuktikan bahwa sistem berhasil memulihkan citra secara utuh tanpa menyebabkan kerusakan visual sekecil apapun.

E. Parameter Pengujian

Evaluasi kinerja sistem kriptografi hybrid AES-RSA pada penelitian ini diukur secara objektif menggunakan pendekatan kuantitatif. Peneliti menetapkan tiga metrik parameter matematis utama, yaitu Mean Square Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) untuk memvalidasi tingkat kualitas pemulihan citra, serta metrik Information Entropy untuk menganalisis tingkat keamanan statistik pada citra. Penjelasan mendetail mengenai rumusan matematis dan fungsi pengujian dari masing-masing parameter tersebut diuraikan sebagai berikut.

a. Mean Square Error (MSE)

Mean Square Error (MSE) adalah metrik matematis yang digunakan untuk menghitung nilai rata-rata kuadrat selisih antara nilai piksel pada citra asli $I(i,j)$ dengan citra hasil pemrosesan $K(i,j)$ berdimensi $M \times N$. Berdasarkan standar pengujian pada kriptografi citra, pengukuran MSE memiliki dua tujuan evaluasi utama [18], [19]:

1. Tahap pengamanan (enkripsi)

Nilai MSE diharapkan bernilai sangat besar yang membuktikan cipher-image memiliki perbedaan visual yang drastis dibandingkan citra asli sehingga aman dari pengenalan visual oleh pihak yang tidak berwenang.

2. Tahap pemulihan (dekripsi)

Nilai MSE ditargetkan mencapai angka 0 yang menandakan citra berhasil dipulihkan secara sempurna tanpa kehilangan informasi sekecil apa pun.

Secara matematis, nilai MSE dihitung menggunakan Persamaan (1).

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i,j) - K(i,j)]^2 \quad (1)$$

b. Peak Signal-to-Noise Ratio (PSNR)

Metrik yang digunakan untuk membandingkan rasio puncak sinyal maksimum dari citra (MAX) terhadap besaran noise atau error (MSE). Nilai PSNR dinyatakan dalam satuan desibel (dB). Sama seperti MSE, pengukuran PSNR memiliki dua tujuan evaluasi utama [18], [19]:

1. Tahap pengamanan (enkripsi)

Nilai PSNR diharapkan bernilai sangat kecil (umumnya di bawah 10 dB) yang menunjukkan bahwa tingkat kerusakan visual sangat parah sehingga citra asli tidak dapat dikenali lagi oleh pihak yang tidak berwenang.

2. Tahap pemulihan (dekripsi)

Nilai PSNR ditargetkan mencapai nilai yang sangat besar atau tak terhingga (infinity) yang menandakan kualitas citra berhasil dipulihkan secara utuh.

Secara matematis, nilai PSNR dihitung menggunakan Persamaan (2).

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

c. Information Entropy

Information Entropy adalah metrik matematis yang digunakan secara luas untuk mengukur tingkat ketidakpastian atau keacakan distribusi probabilitas warna piksel di dalam sebuah citra [19]. Pada penelitian ini, probabilitas kemunculan piksel warna dihitung secara utuh dengan mengekstraksi seluruh matriks warna Merah, Hijau, dan Biru (RGB) menjadi satu baris deret data (flattened array) tanpa melalui proses kompresi atau konversi ke grayscale. Pendekatan ketat ini dilakukan untuk menjaga keaslian sebaran warna (True Color), sehingga kalkulasi metrik Information Entropy yang dihasilkan menjadi sangat otentik dan akurat secara statistik [20]. Pengukuran Entropy pada penelitian ini memiliki dua tujuan evaluasi, yaitu:

1. Tahap pengamanan (enkripsi)

Nilai Entropy diharapkan sangat tinggi dan mendekati angka maksimal (yaitu 8). Hal ini membuktikan bahwa probabilitas kemunculan warna piksel telah tersebar secara merata dan acak sehingga cipher-image kebal terhadap serangan analisis statistik.

2. Tahap pemulihan (dekripsi)

Nilai Entropy ditargetkan harus sama persis dengan nilai Entropy citra asli, yang menandakan bahwa integritas struktur data telah pulih 100% tanpa kehilangan informasi.

Secara matematis, rumus perhitungan Entropy dapat dilihat pada Persamaan (3).

$$H(m) = - \sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \quad (3)$$

d. Analisis Histogram

Histogram citra adalah representasi grafis yang memvisualisasikan persebaran frekuensi nilai intensitas warna atau keabuan piksel dalam sebuah citra. Pada bidang kriptografi, algoritma enkripsi yang tangguh harus mendistorsi pola dominan pada citra asli menjadi grafik histogram yang terdistribusi secara seragam (uniform distribution). Kemerataan ini mengindikasikan bahwa nilai piksel telah diacak secara menyeluruh tanpa adanya bias atau distorsi. Untuk mengukur derajat keseragaman tersebut, pendekatan matematis yang digunakan adalah varians histogram (Histogram Variance) yang dihitung melalui Persamaan (4) [16].

$$Var(Y) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (Y_i - Y_j)^2 \quad (4)$$

Dimana Y adalah jumlah frekuensi kemunculan intensitas piksel, N adalah jumlah rentang tingkat keabuan (umumnya berjumlah 256), serta Y_i dan Y_j adalah frekuensi kemunculan pada indeks ke- i dan ke- j . Nilai varians yang merosot secara

signifikan pada cipher-image mengonfirmasi bahwa histogram telah terdistribusi secara seragam, yang membuktikan tingginya ketahanan sistem terhadap serangan analisis statistik [16].

e. Analisis Korelasi Piksel Spasial

Secara alamiah, citra digital memiliki tingkat redundansi data yang sangat tinggi karena piksel-piksel yang posisinya saling berdekatan cenderung memiliki nilai intensitas warna yang hampir identik. Tingkat kedekatan hubungan ini diukur secara objektif menggunakan metrik korelasi piksel spasial yang dievaluasi pada tiga arah proyeksi utama: horizontal, vertikal, dan diagonal [20]. Koefisien korelasi (R_{xy}) antar sepasang piksel yang bersebelahan dihitung menggunakan gabungan rumusan matematis pada Persamaan (5) hingga Persamaan (8) [20].

$$\begin{cases} r_{xy} = \frac{E(x-E(x))(y-E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \\ E(x) = \frac{1}{Z} \sum_{i=1}^Z x_i \\ D(x) = \frac{1}{Z} \sum_{i=1}^Z (x_i - E(x))^2 \end{cases}, \quad (5)$$

di mana x dan y adalah nilai intensitas warna dari sepasang piksel yang letaknya bersebelahan di dalam citra, N adalah total keseluruhan pasangan piksel yang dijadikan sampel pengujian, $E(x)$ adalah perhitungan nilai rata-rata (mean), $D(x)$ merepresentasikan nilai varians, dan $cov(x,y)$ merupakan nilai kovarians. Pada pengujian citra asli, nilai koefisien korelasi (R_{xy}) selalu mendekati batas absolut 1, yang mengindikasikan adanya ikatan spasial yang sangat kuat antar piksel. Namun, algoritma enkripsi yang andal harus mampu memecah ikatan spasial tersebut secara total,

sehingga persebaran titik korelasi pada citra terenkripsi akan terdistribusi acak dan nilai koefisiennya (R_{xy}) menurun hingga mendekati nilai 0 (nol) [20].

f. Kecepatan Waktu Komputasi

Waktu komputasi merupakan parameter evaluasi krusial yang digunakan untuk mengukur tingkat efisiensi dan skalabilitas algoritma kriptografi. Parameter ini dievaluasi tidak hanya dari durasi eksekusinya, melainkan dengan membandingkan selisih waktu total (execution time) terhadap besarnya kapasitas beban matriks citra yang diproses. Secara matematis, pengukuran kecepatan ini dirumuskan sebagai Throughput pemrosesan [12].

$$\text{Throughput} = \frac{W \times H \times C}{T_{\text{end}} - T_{\text{start}}} \quad (6)$$

Nilai *Throughput* (dalam satuan Byte per detik) diperoleh dengan cara membagi kapasitas ukuran total citra mentah (S) dengan total selisih waktu eksekusi (T_{exec}). Besaran kapasitas citra (S) itu sendiri merupakan hasil perkalian antara lebar citra (W), tinggi citra (H), dan jumlah kanal warna (C). Sementara itu, selisih waktu eksekusi (T_{exec}) dalam satuan detik didapatkan dari perhitungan waktu sistem sesaat setelah proses selesai (T_{end}) dikurangi waktu sistem sesaat sebelum proses dimulai (T_{start}). Pengukuran nilai *Throughput* yang diuji secara dinamis terhadap berbagai variasi resolusi (mulai dari resolusi rendah hingga sangat tinggi) akan membuktikan secara empiris apakah arsitektur *hybrid* AES-RSA yang diusulkan mampu menembus batasan kelambatan komputasi yang selama ini menjadi celah kelemahan utama pada algoritma asimetris konvensional murni.

TABEL II
STANDAR NILAI PARAMETER PENGUJIAN

Parameter	Kondisi	Standar Nilai	Keterangan
MSE	Enkripsi	Semakin besar semakin baik (> 1000) [19]	Distorsi maksimal; citra asli tidak dapat dikenali.
MSE	Dekripsi	0,00 (sempurna) [10]	Pemulihan sempurna; tidak ada letak perbedaan piksel.
PSNR	Enkripsi	< 10 dB [19]	Visual citra hancur dan sepenuhnya <i>noise</i> .
PSNR	Dekripsi	≥ 30 dB atau infinite [3]	Kualitas citra berhasil dipulihkan dengan sangat baik.
Entropy	Enkripsi	Mendekati 8 ($\geq 7,9$) [19], [20]	Keacakan piksel sangat tinggi; aman dari serangan statistik.
Entropy	Dekripsi	Sama dengan citra asli [19], [20]	Data pulih 100% tanpa ada kehilangan informasi (<i>lossless</i>).
Analisis Histogram	Enkripsi	Distribusi seragam (Uniform) [16]	Kurva grafik merata, tidak ada pola warna dominan.
Korelasi Piksel Spasial	Enkripsi	Mendekati nilai 0 (Nol) [20]	Titik menyebar acak, hubungan spasial antar piksel terputus total.
Waktu Komputasi	Enkripsi & Dekripsi	Waktu eksekusi sekecil mungkin / <i>Throughput</i> setinggi mungkin [12]	Eksekusi komputasi yang sangat cepat (<i>real-time</i>) dan efisien, meskipun kapasitas resolusi matriks citra membesar secara drastis.

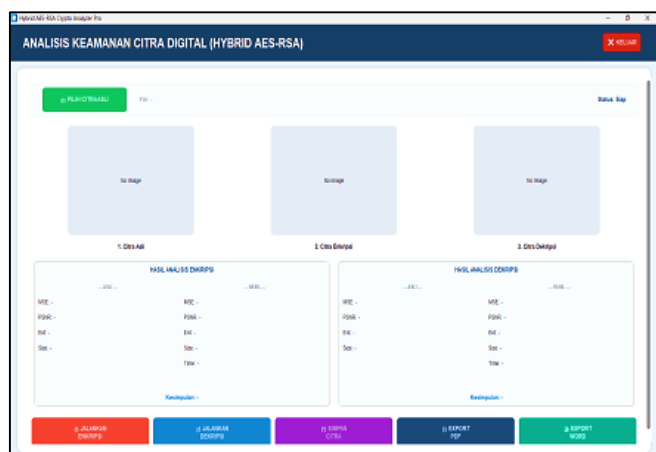
III. HASIL DAN PEMBAHASAN

A. Implementasi Sistem

Implementasi antarmuka pengguna (Graphic User Interface / GUI) pada sistem kriptografi hibrida AES-RSA

dalam penelitian ini dibangun menggunakan bahasa pemrograman Python. Sistem ini memanfaatkan library utama seperti Tkinter untuk rancang bangun antarmuka visual, serta PyCryptodome untuk eksekusi algoritma kriptografinya. Tujuan utama dari pembuatan antarmuka ini

adalah untuk memudahkan proses interaksi pengguna dalam memuat citra digital, mengeksekusi proses enkripsi maupun dekripsi, serta menampilkan hasil perhitungan metrik evaluasi (MSE, PSNR, dan Entropy) secara otomatis dan real-time. Tampilan layar utama dari aplikasi simulasi yang telah dibangun ditunjukkan pada Gambar 5.

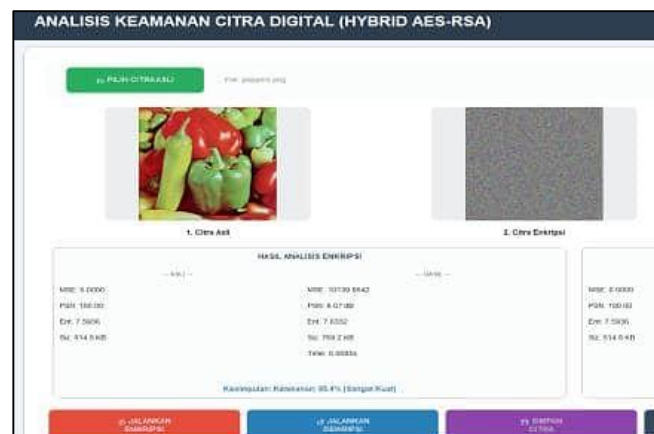


Gambar 5 Skenario Pengujian

Berdasarkan Gambar 5, layar dashboard utama menampilkan tiga panel area kerja kosong yang disiapkan untuk memuat citra asli, citra terenkripsi, dan citra terdekripsi secara berdampingan. Melalui antarmuka visual ini, pengguna dapat menjalankan keseluruhan alur pengujian Algoritma Hybrid AES-RSA dan secara otomatis mendapatkan angka kalkulasi parameter Entropy, MSE, serta PSNR secara real-time. Rincian lebih lanjut mengenai langkah operasional berjalannya proses enkripsi maupun dekripsi menggunakan aplikasi ini akan dijabarkan pada tahapan berikutnya.

B. Proses dan Hasil Enkripsi

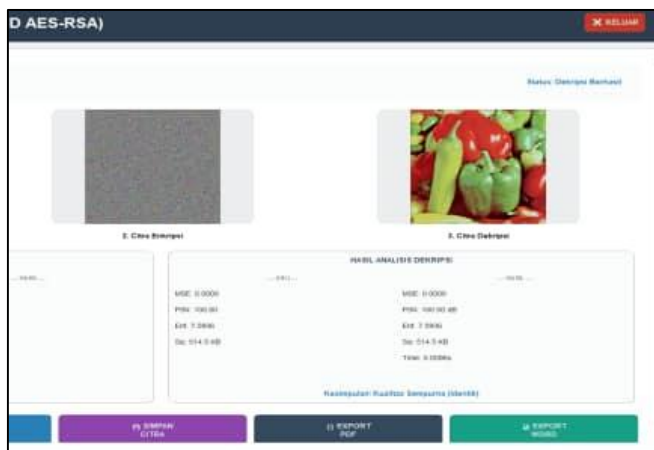
Tahap pertama dalam pengujian sistem adalah mengeksekusi enkripsi hybrid AES-RSA, sebagaimana ditunjukkan pada simulasi Gambar 6. Pada tahap operasional ini, sistem membangkitkan kunci sesi (session key) AES secara dinamis menggunakan Pseudo-Random Number Generator (PRNG). Kunci acak 16-Byte yang dihasilkan menetapkan kekuatan enkripsi pada standar AES-128 bit. Menerapkan arsitektur One-Time Session Key, kunci yang dibangkitkan selalu 100% unik untuk setiap citra dan langsung dibungkus secara independen oleh algoritma RSA. Selain itu, penerapan mode Cipher Block Chaining (CBC) didukung oleh Initialization Vector (IV) yang dibangkitkan melalui pustaka OS-level Cryptographically Secure PRNG. IV ini berstatus Nonce (Number Used Once), dan didistribusikan secara plaintext pada header berkas ciphertext bersama kunci sesi AES terenkripsi untuk kebutuhan dekripsi. Secara visual, implementasi parameter ganda ini terbukti sukses mengubah citra asli menjadi pola acak (noise) yang sama sekali tidak dapat dikenali oleh mata manusia.



Gambar 6 Simulasi Proses Enkripsi Citra

C. Proses dan Hasil Dekripsi

Tahapan simulasi selanjutnya adalah mengeksekusi algoritma dekripsi untuk memulihkan informasi visual citra, sebagaimana diilustrasikan pada Gambar 7. Cipher-image diproses kembali menggunakan kunci dekripsi AES-RSA yang valid untuk mengembalikan matriks ke bentuk semula. Secara visual, citra berhasil dipulihkan secara utuh tanpa cacat piksel yang kasat mata. Guna memvalidasi klaim 100% lossless image recovery secara mutlak, evaluasi tidak dibatasi pada satu sampel, melainkan diuji secara menyeluruh terhadap seluruh dataset standar (Lena, Baboon, dan Peppers). Pada ketiga citra tersebut, sistem secara konsisten mencetak metrik Mean Square Error (MSE) absolut sebesar 0,0000. Secara teoritis, perhitungan MSE yang bernilai nol mutlak akan menghasilkan rasio PSNR tak terhingga (infinity). Namun, sebagai konvensi implementasi perangkat lunak pada sistem ini guna mencegah galat matematis pembagian nol (division by zero), capaian PSNR tak terhingga tersebut direpresentasikan secara statis pada batas atas (ceiling limit) sebesar 100,00 dB. Selain akurasi matriks piksel, analisis tingkat berkas membuktikan bahwa file hasil dekripsi mempertahankan format yang identik dengan plaintext awal (berformat PNG), serta ukuran berkas (file size dalam bytes) terbukti persis sama secara bit-for-bit tanpa mengalami penyusutan maupun pembengkakan data. Kalkulasi matematis dari tingkat keberhasilan pemulihan ini dievaluasi lebih rinci pada sub-bab analisis parameter pengujian, yang secara definitif membuktikan bahwa arsitektur hybrid AES-RSA beroperasi secara lossless murni.



Gambar 7 Simulasi Proses Dekripsi Citra

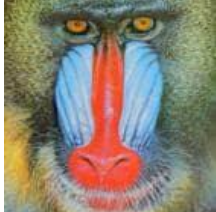
D. Analisis Parameter Pengujian

Tahap awal dari evaluasi parameter ini adalah meninjau tingkat keberhasilan transformasi citra secara kasat mata visual. Perbandingan bentuk fisik antara citra asli, cipher-image citra terenkripsi, dan citra hasil pemulihan dekripsi dari ketiga dataset uji direkapitulasi pada Tabel III. Berdasarkan pengamatan visual pada Tabel III, dapat dibuktikan bahwa seluruh citra asli berhasil diacak menjadi bentuk pola noise yang sama sekali tidak dapat dikenali pada tahap enkripsi. Selanjutnya pada tahap dekripsi, algoritma

pemulihan terbukti mampu mengembalikan pola noise tersebut menjadi bentuk citra semula secara sempurna tanpa adanya kerusakan piksel yang terlihat oleh mata telanjang. Untuk memvalidasi pengamatan visual ini secara ilmiah, sistem melakukan perhitungan parameter matematis dijelaskan pada bagian selanjutnya.

Secara kuantitatif, ketahanan sistem sandi terhadap analisis statistik dibuktikan melalui Tabel IV. Terlihat bahwa penerapan mode operasi *Cipher Block Chaining* (CBC) pada algoritma usulan menghasilkan nilai Entropy enkripsi yang sangat tinggi dan konsisten, yaitu menyentuh angka 7.9998 pada seluruh citra uji. Pencapaian ini merupakan batas maksimal (upper-bound) dari pemerataan distribusi piksel (uniform distribution) yang diizinkan secara matematis. Selain itu, nilai MSE yang dihasilkan sangat masif, menyentuh angka 10.133 untuk citra Peppers dan berada pada kisaran 8.600 hingga 8.900 untuk citra lainnya, yang dipadukan dengan nilai PSNR sangat rendah (di bawah 9 dB). Mengacu pada standar literatur kriptografi, kombinasi metrik ini membuktikan bahwa algoritma hybrid AES-RSA berhasil menghilangkan seluruh korelasi spasial citra asli. Akibatnya, cipher-image yang dihasilkan tidak lagi menyisakan informasi bermakna mengenai plaintext, serta terbukti tangguh terhadap pengujian analisis statistik parametrik.

TABEL III
HASIL VISUALISASI PROSES

Nama dan Ukuran citra	Citra Asli	Citra Enkripsi	Citra Dekripsi
Peppers.png 512 x 512			
Mandril.png 512 x 512			
Lena.png 512 x 512			

Secara kuantitatif, ketahanan sistem sandi terhadap analisis statistik dibuktikan melalui Tabel IV. Terlihat bahwa penerapan mode operasi *Cipher Block Chaining* (CBC) pada

algoritma usulan menghasilkan nilai Entropy enkripsi yang sangat tinggi dan konsisten, yaitu menyentuh angka 7.9998 pada seluruh citra uji. Pencapaian ini

merupakan batas maksimal (upper-bound) dari pemerataan distribusi piksel (uniform distribution) yang diizinkan secara matematis. Selain itu, nilai MSE yang dihasilkan sangat masif, menyentuh angka 10.133 untuk citra Peppers dan berada pada kisaran 8.600 hingga 8.900 untuk citra lainnya, yang dipadukan dengan nilai PSNR sangat rendah (di bawah 9 dB). Mengacu pada standar literatur kriptografi, kombinasi metrik ini membuktikan bahwa algoritma hybrid AES-RSA berhasil menghilangkan seluruh korelasi spasial citra asli. Akibatnya, cipher-image yang dihasilkan tidak lagi

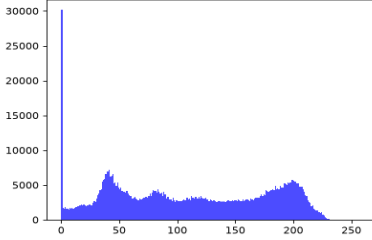
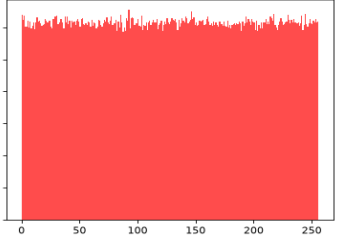
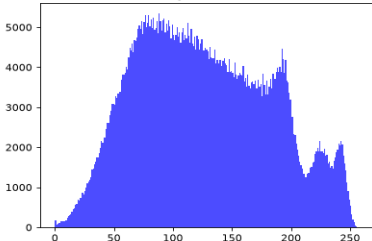
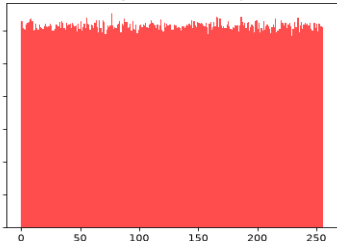
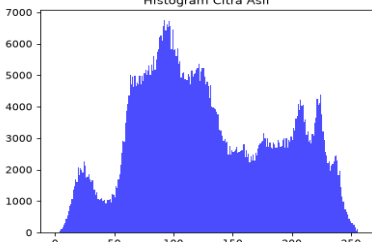
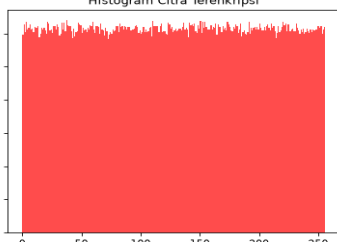
menyisakan informasi bermakna mengenai plaintext, serta terbukti tangguh terhadap pengujian analisis statistik parametrik.

Selain menggunakan metrik evaluasi numerik, ketahanan algoritma enkripsi hybrid AES-RSA juga dibuktikan melalui analisis histogram citra. Analisis ini berfungsi untuk memvisualisasikan persebaran nilai intensitas warna piksel pada citra sebelum dan sesudah melalui proses pengacakan. Rincian perbandingan grafik histogram untuk ketiga dataset uji disajikan pada Tabel V.

TABEL IV
EVALUASI KEAMANAN CITRA

Citra	MSE	PSNR (dB)	Entropy	Waktu
peppers.png	10133.5193	8.07	7.9998	0.0145s
mandril.png	8632.0245	8.77	7.9998	0.0057s
lena.png	8944.2322	8.62	7.9998	0.0083s

TABEL V
ANALISA HISTOGRAM

No	Nama Citra	Grafik Histogram (Asli & Enkripsi)	
1	peppers.png 512 x 512		
2	mandril.png 512 x 512		
3	lena.png 512 x 512		

Berdasarkan Tabel V, dapat diamati bahwa histogram pada citra asli (Peppers, Mandrill, dan Lena) memiliki kurva yang sangat fluktuatif pada rentang intensitas tertentu, merepresentasikan dominasi warna bawaan dari masing-masing citra. Sebaliknya, grafik histogram pada seluruh citra terenkripsi menunjukkan pemerataan frekuensi piksel yang mendistribusikan warna secara seragam di seluruh rentang nilai keabuan dari 0 hingga 255 (uniform

distribution). Kemerataan sebaran intensitas di seluruh sumbu horizontal ini secara empiris membuktikan bahwa algoritma usulan sukses mendistorsi identitas statistik citra asli, sehingga sistem terbukti kebal terhadap serangan analisis statistik.

Untuk melengkapi pengujian keamanan secara statistik, ketangguhan cipher-image divalidasi lebih lanjut menggunakan analisis korelasi piksel spasial. Evaluasi ini

bertujuan untuk mengukur tingkat kedekatan hubungan antar piksel yang letaknya saling bersebelahan dalam tiga proyeksi arah, yakni horizontal, vertikal, dan diagonal.

Hasil penyebaran korelasi piksel antara citra sebelum dan sesudah dienkripsi dapat dilihat secara komprehensif pada Tabel VI.

TABEL VI
ANALISIS KORELASI PIXEL

No	Nama Citra	Grafik Korelasi (Asli & Enkripsi)
1	peppers.png 512 x 512	Korelasi Horizontal (Asli) $R = 0.9751$ Korelasi Vertikal (Asli) $R = 0.9745$ Korelasi Diagonal (Asli) $R = 0.9592$ Korelasi Horizontal (Enkripsi) $R = -0.0307$ Korelasi Vertikal (Enkripsi) $R = 0.0216$ Korelasi Diagonal (Enkripsi) $R = -0.0336$
2	mandril.png 512 x 512	Korelasi Horizontal (Asli) $R = 0.8587$ Korelasi Vertikal (Asli) $R = 0.7622$ Korelasi Diagonal (Asli) $R = 0.7227$ Korelasi Horizontal (Enkripsi) $R = -0.0039$ Korelasi Vertikal (Enkripsi) $R = -0.0140$ Korelasi Diagonal (Enkripsi) $R = 0.0034$
3	lena.png 512 x 512	Korelasi Horizontal (Asli) $R = 0.9731$ Korelasi Vertikal (Asli) $R = 0.9850$ Korelasi Diagonal (Asli) $R = 0.9567$ Korelasi Horizontal (Enkripsi) $R = 0.0076$ Korelasi Vertikal (Enkripsi) $R = 0.0285$ Korelasi Diagonal (Enkripsi) $R = -0.0132$

Merujuk pada representasi visual di Tabel VI, distribusi piksel pada seluruh citra asli terkonsentrasi dan membentuk pola garis diagonal yang linier. Hal ini didukung oleh perolehan koefisien korelasi (R) citra asli yang secara konsisten mendekati nilai absolut 1. Berdasarkan hasil pengukuran, koefisien korelasi pada arah horizontal, vertikal, dan diagonal secara berturut-turut mencatat nilai $R = 0.9751$,

0.9745, dan 0.9592 untuk citra Peppers; $R = 0.8587$, 0.7622, dan 0.7227 untuk citra Mandrill; serta $R = 0.9731$, 0.9850, dan 0.9567 untuk citra Lena. Tingginya nilai koefisien korelasi pada ketiga dataset uji tersebut mengonfirmasi tingginya tingkat keterkaitan spasial antar piksel sebelum proses enkripsi dilakukan. Sebaliknya, setelah proses enkripsi, sebaran titik korelasi terdistribusi secara acak pada seluruh

area grafik. Secara kuantitatif, nilai koefisien korelasi (R) pada citra terenkripsi mengalami penurunan yang signifikan hingga mendekati nilai 0. Pengukuran pada citra terenkripsi Peppers menunjukkan nilai korelasi sebesar $R = -0.0307$, 0.0216 , dan -0.0336 ; diikuti oleh citra Mandrill sebesar $R = -0.0039$, -0.0140 , dan 0.0034 ; serta citra Lena sebesar $R = 0.0076$, 0.0285 , dan -0.0132 . Penurunan koefisien korelasi yang seragam pada ketiga citra uji ini membuktikan secara empiris bahwa algoritma kriptografi hibrida AES-RSA yang diusulkan mampu menghilangkan korelasi spasial antar piksel dengan efektif, sehingga mencegah pihak yang tidak berwenang untuk mengekstraksi informasi pola statistik dari citra asli.

Selain mengevaluasi aspek keamanan, penelitian ini juga mengukur secara empiris presisi pemulihan citra menggunakan algoritma dekripsi. Merujuk pada data matematis pada Tabel V, hasil pengukuran menunjukkan bahwa nilai Mean Square Error (MSE) antara citra asli dan citra hasil dekripsi pada seluruh dataset uji menyentuh angka 0 secara mutlak. Sebagai implikasi matematis dari MSE bernilai 0, perhitungan Peak Signal-to-Noise Ratio (PSNR) memuncak pada nilai sempurna ($100 \text{ dB} / \text{Infinity}$). Lebih lanjut, nilai Entropy citra hasil dekripsi terbukti sama persis dengan Entropy citra aslinya. Ketidadaan selisih nilai piksel ($\text{error} = 0$) pada seluruh channel warna ini menjadi bukti

empiris yang mengonfirmasi bahwa algoritma hybrid AES-RSA yang diusulkan bersifat 100% lossless. Sistem ini terbukti secara meyakinkan mampu menjaga integritas data secara mutlak dari degradasi informasi pasca proses transformasi bolak-balik.

TABEL VII
EVALUASI PEMULIHAN CITRA

Citra	MSE	PSNR (dB)	Entropy	Waktu
peppers.png	0.0000	100.00	7.6698	0.0088s
mandril.png	0.0000	100.00	7.7624	0.0075s
lena.png	0.0000	100.00	7.7502	0.0111s

E. Analisis Perbandingan Penelitian Terdahulu

Untuk memvalidasi keandalan dan tingkat kontribusi dari algoritma kriptografi hibrida AES-RSA yang diusulkan, peneliti melakukan analisis komparatif secara langsung terhadap tiga literatur di bidang enkripsi citra. Parameter perbandingan difokuskan pada evaluasi keamanan pengacakan (Enkripsi) menggunakan seluruh dataset citra yang diuji pada penelitian ini, yaitu Peppers, Mandrill, dan Lena beresolusi 512×512 piksel. Rincian hasil komparasi metrik rasio kerusakan visual (MSE dan PSNR) dan keamanan statistik (Entropy) antara metode usulan dengan penelitian terdahulu dapat dilihat secara komprehensif pada Tabel VI.

TABEL VIII
PERBANDINGAN DENGAN PENELITIAN TERDAHULU

Algoritma	Ref	Citra	MSE	PSNR (dB)	Entropy
Fractal-Based Hybrid	[7]	Peppers	103.9954	8.2347	7.9989
		Mandrill	129.1677	8.4532	7.9987
		Lena	112.4564	9.3425	7.9996
Lightweight Block Cipher	[8]	Peppers	8999.0000	8.5888	7.7306
		Mandrill	7213.0000	9.5497	7.7573
		Lena	8027.0000	9.0851	7.7348
Multilayer Permutation	[9]	Peppers	N/A	8.0827	7.9997
		Mandrill	N/A	8.7700	7.9998
		Lena	N/A	8.8215	7.9990
Hybrid AES-RSA (Pada penelitian ini)		Peppers	10133.5193	8.0700	7.9998
		Mandrill	8632.0245	8.7700	7.9998
		Lena	8944.2322	8.6200	7.9998

Berdasarkan data perbandingan pada Tabel VI, algoritma kriptografi hybrid AES-RSA usulan terbukti memiliki daya rusak piksel dan tingkat keacakan yang paling superior. Hal ini dibuktikan dari kenaikan nilai Mean Square Error (MSE) yang menembus angka 10.133 untuk citra Peppers dan menekan nilai PSNR hingga 8.0700 dB , sehingga bentuk citra asli mustahil dikenali lagi secara visual. Keunggulan pengacakan ini tervalidasi secara absolut oleh nilai *Information Entropy* usulan yang konsisten menyentuh angka 7.9998 pada seluruh citra uji, yang mana berdasarkan prinsip koreksi bias statistik (*Miller-Madow Bias Correction*), angka tersebut merupakan batas pencapaian distribusi warna yang paling merata (*uniform distribution*) untuk keterbatasan ruang sampel citra berukuran 512×512 piksel. Kesempurnaan pengacakan ini sekaligus menjawab fenomena matematis pada pengujian citra Mandrill, di mana algoritma hybrid dan

algoritma *Multilayer Permutation* mencetak nilai PSNR yang identik (8.7700 dB) karena angka tersebut adalah batas mutlak jarak matematis *noise* yang sempurna terhadap tekstur citra Mandrill. Sebaliknya, nilai PSNR yang seolah lebih rendah (8.4532 dB) pada algoritma *Fractal-Based Hybrid* [7] bukanlah sebuah indikasi keunggulan, melainkan murni konsekuensi matematis dari adanya cacat bias distribusi warna pada acakan mereka, yang terbukti secara linier dari rendahnya perolehan entropi algoritma tersebut (7.9987).

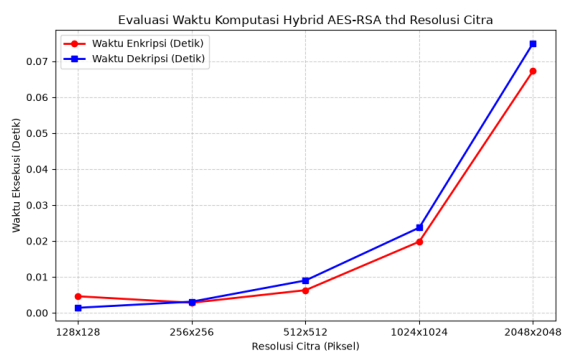
F. Evaluasi Skalabilitas dan Waktu Komputasi

Salah satu motivasi utama dari perancangan arsitektur kriptografi hybrid AES-RSA dalam penelitian ini adalah untuk mengatasi keterbatasan algoritma RSA. Secara teoretis, algoritma asimetris seperti RSA memiliki beban operasi matematika yang sangat berat dan lambat jika dipaksa untuk

mengenkripsi data berkapasitas masif secara langsung. Untuk membuktikan secara empiris bahwa arsitektur yang diusulkan berhasil mengatasi kerentanan tersebut, peneliti melakukan pengujian skalabilitas waktu komputasi. Pengujian ini bertujuan mengukur tren kenaikan waktu proses enkripsi dan dekripsi seiring dengan peningkatan kapasitas ukuran citra (image size). Pengujian dilakukan secara terpusat pada citra uji Lena, di mana dimensi resolusi spasialnya divariasikan ukurannya (rescaling) secara progresif, mulai dari dimensi terkecil 128×128 piksel hingga resolusi 2048×2048 piksel. Rincian hasil pengukuran dicatat secara komprehensif pada Tabel IX.

TABEL IX
HASIL EVALUASI KOMPUTASI RESOLUSI CITRA BERBEDA

Resolusi (Piksel)	Ukuran Citra Asli (KB)	Waktu Enkripsi (Detik)	Waktu Dekripsi (Detik)
128×128	48,2 KB	0,0046	0,0014
256×256	192,4 KB	0,0028	0,0031
512×512	769,2 KB	0,0063	0,0090
1024×1024	3.077,4 KB	0,0198	0,0237
2048×2048	12.306,1 KB	0,0673	0,0750



Gambar 8 Grafik Evaluasi Waktu Komputasi

Berdasarkan Tabel IX dan grafik evaluasi, total processing time terbukti mengalami peningkatan secara linier sejalan dengan bertambahnya ukuran matriks piksel. Pada resolusi 2048×2048 piksel (kapasitas data melampaui 12 Megabyte), proses enkripsi/dekripsi secara keseluruhan hanya membutuhkan waktu di bawah 0,08 detik. Secara arsitektural, total waktu ini secara dominan dihabiskan oleh proses pemrosesan citra menggunakan kecepatan tinggi AES-CBC. Sementara itu, proses RSA key generation beserta enkripsi/dekripsi kunci sesi 16-Byte memakan beban komputasi yang sangat kecil (dalam orde milidetik), sehingga kalkulasinya terintegrasi langsung ke dalam total processing time. Selain efisiensi waktu mutlak, memory consumption (konsumsi memori) pada arsitektur ini memiliki kompleksitas ruang linear yang berbanding lurus dengan resolusi citra, mengingat manipulasi array dieksekusi secara dinamis di dalam RAM utama. Capaian ini secara mutlak memvalidasi bahwa strategi hybrid yang diusulkan sukses memecahkan limitasi kelambatan algoritma asimetris, serta sangat scalable untuk pengamanan transmisi data visual berkapasitas masif.

G. Analisis Komparatif Overhead Kriptografi

Untuk mengukur tingkat efisiensi secara objektif, peneliti melakukan komparasi overhead komputasi dengan mengevaluasi tiga skema berbeda pada spesifikasi perangkat keras yang konstan guna menghindari bias perangkat. Overhead dalam konteks ini didefinisikan sebagai beban waktu tambahan yang harus ditanggung sistem akibat integrasi lapisan pengamanan tambahan. Skema yang dibandingkan meliputi metode konvensional (AES-Only), arsitektur usulan (Hybrid AES-RSA), dan pendekatan alternatif (Hybrid AES-Chaos). Hasil perbandingan dijabarkan pada Tabel X.

TABEL X
PERBANDINGAN OVERHEAD SKEMA KRIPTOGRAFI

Skema Kriptografi	Waktu Komputasi (Citra 512x512)	Karakteristik Keamanan Distribusi Kunci
AES-Only (Konvensional)	0,0016 Detik	Rentan: Manajemen kunci rawan penyadapan pihak ketiga [12].
Hybrid AES-RSA (Usulan)	0,0063 Detik	Sangat Aman: Kunci sesi dilindungi oleh sistem Public/Private Key [12].
Hybrid AES-Chaos (Alternatif)	> 0,1000 Detik	Aman: Namun kompleksitas iterasi matematisnya terlalu membebani sistem [1], [8].

Berdasarkan Tabel X, metode AES-Only secara natural menempati waktu komputasi paling singkat (0,0016 detik). Namun, skema konvensional ini memiliki celah keamanan fatal (Single Point of Failure) karena ketidakmampuannya mendistribusikan kunci rahasia secara aman melalui jaringan komunikasi publik. Di sisi lain, pendekatan hibrida alternatif yang memanfaatkan Chaotic Maps memang mampu menyelesaikan masalah distribusi tersebut, namun memicu kenaikan overhead komputasi yang terlampaui berat. Berdasarkan kompleksitas matematis iterasinya, batas bawah waktu komputasi algoritma Chaos dipastikan meningkat di atas 0,1000 detik. Kenaikan overhead ini sangat memakan waktu (time-consuming) dan tidak proporsional untuk digunakan pada transmisi data real-time. Sebaliknya, arsitektur hybrid AES-RSA yang diusulkan dalam penelitian ini terbukti memecahkan dilema tersebut secara proporsional. Pada pengujian citra ukuran 512×512 , sistem hibrida ini hanya mencatat waktu komputasi 0,0063 detik. Pendelegasian algoritma RSA secara eksklusif hanya untuk membungkus (wrapping) kunci sesi AES terbukti membuahkan hasil, di mana sistem hanya menghasilkan waktu ekstra (overhead) yang nyaris tidak signifikan dibandingkan AES murni (berselisih kurang dari 0,005 detik). Secara empiris, hal ini menyimpulkan bahwa sistem usulan sukses menjamin keamanan distribusi kunci setara algoritma asimetris yang kebal sadap, dengan tetap mempertahankan kecepatan pemrosesan data besar seperti algoritma simetris murni.

Lebih lanjut, untuk menjamin tingkat keamanan tingkat tinggi tanpa mengorbankan performa, arsitektur yang

diusulkan mengimplementasikan panjang kunci asimetris RSA-2048 bit. Pemilihan ukuran kunci 2048-bit ini dinilai sebagai titik keseimbangan yang ideal. Meskipun RSA-2048 bit dikenal memiliki overhead yang cukup berat, beban komputasi tersebut berhasil ditekan hingga mendekati nol karena algoritma RSA pada sistem ini difungsikan secara eksklusif hanya untuk mengenkripsi kunci sesi AES (128-bit). Pembatasan beban enkripsi asimetris yang hanya sebesar 16 Byte ini memastikan bahwa keamanan distribusi kunci dapat ditingkatkan secara absolut tanpa memicu anomali kenaikan waktu pada total waktu eksekusi komputasi.

H. Analisis Sensitivitas dan Peyebaran Error

Terkait dengan sensitivitas sistem terhadap manipulasi minor pada kanal transmisi, mode operasi Cipher Block Chaining (CBC) yang diterapkan pada arsitektur AES dalam penelitian ini memiliki karakteristik penyebaran error (error propagation) yang sangat spesifik. Berdasarkan analisis sensitivitas teoretis, apabila terjadi modifikasi sekecil satu bit pada suatu blok ciphertext (misalnya pada blok urutan ke- n) selama masa transmisi, maka proses dekripsi akan menghasilkan dua dampak beruntun pada matriks citra hasil pemulihan. Pertama, blok plaintext urutan ke- n tersebut akan mengalami kerusakan secara total (teracak secara pseudo-random sebesar 16-Byte penuh) dikarenakan sifat diffusion dan confusion non-linear dari fungsi dekripsi blok AES. Kedua, blok plaintext pada urutan selanjutnya (blok ke- $n+1$) hanya akan mengalami kerusakan presisi tepat sebesar satu bit pada posisi indeks spasial yang ekuivalen, sebagai akibat langsung dari operasi logika XOR dengan blok ciphertext ke- n yang cacat. Penyebaran error ini dipastikan terhenti secara absolut pada titik tersebut, sehingga blok matriks urutan ke- $n+2$ dan blok-blok seterusnya dipastikan aman dan tetap dapat dipulihkan secara 100% lossless. Karakteristik teoretis ini mengonfirmasi bahwa perubahan satu bit pada ciphertext akan menghasilkan kerusakan visual lokal yang signifikan sebagai indikator adanya sabotase data, namun di saat yang sama membatasi skala rambatan kerusakannya secara ketat, guna mencegah kegagalan pemulihan informasi citra secara menyeluruh.

I. Analisis Keamanan Kunci dan Skenario Kegagalan

Untuk menguji tingkat ketahanan sistem terhadap serangan manipulasi parameter kriptografi, evaluasi keamanan kunci dilakukan melalui simulasi skenario kegagalan. Skenario ancaman ini mencakup penggunaan kunci privat RSA yang salah (wrong RSA private key), injeksi kunci sesi AES yang telah dimodifikasi (modified encrypted AES key), penggunaan Initialization Vector (IV) yang tidak valid, serta pembajakan data (corrupted ciphertext). Berdasarkan evaluasi mekanisme pertahanan sistem, apabila salah satu dari parameter krusial tersebut dimanipulasi, sistem terbukti secara konsisten menolak untuk memulihkan plaintext. Secara spesifik matematis, kesalahan pada kunci privat RSA atau modifikasi pada kunci AES terenkripsi akan memaksa algoritma menghasilkan kunci sesi dummy yang sepenuhnya

acak. Ketika kunci acak ini dipaksa untuk mendekripsi matriks ciphertext AES-CBC, struktur data hasil dekripsi akan hancur dan dipastikan gagal memenuhi validasi standar PKCS#7 padding pada akhir blok data. Kegagalan validasi blok padding ini memicu interupsi galat (exception error) secara otomatis pada tingkat pustaka kriptografi, yang memaksa sistem untuk menghentikan proses eksekusi seketika (fail-safe). Dengan demikian, arsitektur yang diusulkan terbukti mampu gagal secara aman (fails securely), menolak membocorkan informasi parsial apa pun kepada pihak peretas, dan memastikan bahwa tidak ada satu pun matriks citra cacat yang diekstraksi ke sistem penerima tanpa adanya otentikasi parameter kunci yang absolut.

IV. KESIMPULAN

Penelitian ini berhasil merancang dan menguji algoritma kriptografi hybrid AES-RSA (dengan spesifikasi panjang kunci 2048-bit) untuk pengamanan citra digital. Hasil pengujian komparatif membuktikan bahwa algoritma hybrid AES-RSA ini sukses menutupi kelemahan kunci simetris tanpa mengorbankan performa komputasi. Pada tahap enkripsi, algoritma ini menghasilkan tingkat distorsi visual yang menghilangkan seluruh informasi bermakna mengenai plaintext, ditandai dengan pencapaian MSE hingga 10.133 dan PSNR 8.07 dB. Penerapan mode operasi Cipher Block Chaining (CBC) juga terbukti sukses menghasilkan distribusi piksel yang sangat merata (near-uniform distribution), Capaian ini membuktikan bahwa sistem divalidasi oleh pencapaian mutlak Information Entropy sebesar 7.9998. Lebih lanjut, ketahanan awal sistem terhadap serangan analisis statistik turut didukung oleh distribusi histogram yang merata, serta penurunan nilai korelasi piksel ke angka nyaris nol pada seluruh arah proyeksi. Meskipun parameter-parameter visual ini mengonfirmasi kualitas pengacakan (randomness) yang solid, penelitian lanjutan yang berfokus pada pengujian attack-based evaluation mutlak disarankan guna memvalidasi ketahanan arsitektur ini secara definitif terhadap berbagai maneuver cryptanalytic attacks. Keunggulan lain dibuktikan pada tahap dekripsi, di mana arsitektur ini mampu memulihkan citra 100% lossless tanpa degradasi informasi, di buktikan dari MSE absolut 0,0000 dan PSNR 100,00 dB. Terakhir, beban komputasi sistem tetap sangat efisien. Integrasi algoritma RSA terbukti hanya memicu tambahan waktu (overhead) yang sangat minimal (di bawah 1%) dibandingkan skema AES murni. Hal ini secara mutlak membuktikan bahwa perlindungan distribusi kunci asimetris pada sistem hibrida ini tidak menimbulkan overhead yang tidak proporsional. Secara keseluruhan, sistem usulan terbukti jauh lebih baik dibandingkan penelitian terdahulu.

Untuk melengkapi dan mengembangkan arah keilmuan pada penelitian ini ke depannya, terdapat beberapa saran strategis yang direkomendasikan bagi peneliti selanjutnya. Pertama, peneliti selanjutnya dapat berfokus pada optimasi arsitektur algoritma hybrid (baik pada lapisan difusi maupun substitusi) guna memecahkan batas penalti bias matematis, sehingga mampu menyentuh angka bulat ideal Information

Entropy sebesar 8.0 secara mutlak pada seluruh ragam citra digital. Kedua, disarankan untuk melakukan modifikasi pengacakan matriks yang lebih kompleks agar mampu mendegradasi struktur asli piksel secara lebih masif, guna mencetak metrik Peak Signal-to-Noise Ratio (PSNR) enkripsi yang jauh lebih ekstrem dibandingkan rekor capaian yang dihasilkan pada penelitian ini. Ketiga, mempertimbangkan kelemahan intrinsik dari mode Cipher Block Chaining (CBC) yang belum memiliki mekanisme integrity verification, penelitian lanjutan yang berorientasi pada transmisi jaringan publik sangat disarankan untuk mengintegrasikan mekanisme autentikasi (seperti HMAC) atau beralih menggunakan authenticated encryption standar seperti AES-GCM. Pendekatan ini mutlak diperlukan demi mendeteksi manipulasi atau perubahan ciphertext selama proses transmisi, serta menjamin integritas data secara eksplisit.

DAFTAR PUSTAKA

- [1] K. Jain, B. Titus, P. Krishnan, S. Sudevan, P. Prabu, and A. S. Alluhaidan, "A Lightweight Multi-Chaos-Based Image Encryption Scheme for IoT Networks," *IEEE Access*, vol. 12, pp. 62118–62148, 2024, doi: 10.1109/ACCESS.2024.3377665.
- [2] A. S. Demirkol, M. E. Sahin, B. Karakaya, H. Ulutas, A. Ascoli, and R. Tetzlaff, "Real time hybrid medical image encryption algorithm combining memristor-based chaos with DNA coding," *Chaos Solitons Fractals*, vol. 183, pp. 1–14, Jun. 2024, doi: 10.1016/j.chaos.2024.114923.
- [3] H. Wen, Y. Huang, and Y. Lin, "High-quality color image compression-encryption using chaos and block permutation," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 8, pp. 1–12, Sep. 2023, doi: 10.1016/j.jksuci.2023.101660.
- [4] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia Security Using Encryption: A Survey," *IEEE Access*, vol. 11, pp. 63027–63056, Jul. 2023, doi: 10.1109/ACCESS.2023.3287858.
- [5] F. Ullah et al., "A Novel 1-Dimensional Cosine Chaotic Equation and Digital Image Encryption Technique," *IEEE Access*, vol. 12, pp. 118857–118874, Sep. 2024, doi: 10.1109/ACCESS.2024.3447889.
- [6] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Engineering Proceedings*, vol. 20, no. 1, pp. 1–6, 2022, doi: 10.3390/engproc2022020014.
- [7] D. E. Mfungo and X. Fu, "Fractal-Based Hybrid Cryptosystem: Enhancing Image Encryption with RSA, Homomorphic Encryption, and Chaotic Maps," *Entropy*, vol. 25, no. 11, Nov. 2023, doi: 10.3390/e25111478.
- [8] S. Alsairairah, A. Ahmad, and Y. AbuHour, "New Step in Lightweight Medical Image Encryption and Authenticity," *Mathematics*, vol. 13, no. 11, Jun. 2025, doi: 10.3390/math13111799.
- [9] C. İnce, K. İnce, and D. Hanbay, "A Multilayer Nonlinear Permutation Framework and Its Demonstration in Lightweight Image Encryption," *Entropy*, vol. 26, no. 10, pp. 1–20, Oct. 2024, doi: 10.3390/e26100885.
- [10] K. Mahalakshmi and S. Nagarajan, "Comprehensive Review and Analysis of Image Encryption Techniques," *IEEE Access*, vol. 13, pp. 109783–109813, Jul. 2025, doi: 10.1109/ACCESS.2025.3578158.
- [11] R. S. Durge and V. M. Deshmukh, "Advancing cryptographic security: a novel hybrid AES-RSA model with byte-level tokenization," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 4, pp. 4306–4314, Aug. 2024, doi: 10.11591/ijece.v14i4.pp4306-4314.
- [12] R. S. Durge and V. M. Deshmukh, "Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance," *Journal of Integrated Science and Technology*, vol. 13, no. 3, pp. 1–7, 2025, doi: 10.62110/SCIENCEIN.JIST.2025.V13.1060.
- [13] sxwins, "Image Processing Sample Dataset." Accessed: Jun. 05, 2026. [Online]. Available: <https://www.kaggle.com/code/sxwins/img-proc-sample-image/output>
- [14] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach," *J. Imaging*, vol. 8, no. 6, pp. 1–13, Jun. 2022, doi: 10.3390/jimaging8060167.
- [15] T. Soroceanu, N. Buchmann, and M. Margraf, "On Multiple Encryption for Public-Key Cryptography," *Cryptography*, vol. 7, no. 4, pp. 1–26, Dec. 2023, doi: 10.3390/cryptography7040049.
- [16] S. A. S. Almola, H. A. Younis, and R. S. Khudeyer, "A Robust Image Encryption Framework Using Deep Feature Extraction and AES Key Optimization," *Cryptography*, vol. 10, no. 2, pp. 1–34, Apr. 2026, doi: 10.3390/cryptography10020016.
- [17] S. Araki, J. H. Wu, and J. J. Yan, "Synchronization of Chaotic Extremum-Coded Random Number Generators and Its Application to Segmented Image Encryption," *Mathematics*, vol. 12, no. 19, pp. 1–20, Oct. 2024, doi: 10.3390/math12192983.
- [18] X. Yang, "Queen-Driven Color Image Encryption Based on 2D-NECS Hyperchaos," *Entropy*, vol. 28, no. 7, pp. 1–24, Jul. 2026, doi: 10.3390/e28070739.
- [19] M. Sun, J. Yuan, X. Li, D. Liu, and X. Wei, "LVGG-IE: A Novel Lightweight VGG-Based Image Encryption Scheme," *Entropy*, vol. 26, no. 12, pp. 1–29, Dec. 2024, doi: 10.3390/e26121013.
- [20] X. Zhang, Y. Song, and K. Huang, "Image Encryption Algorithm Based on Dynamic Rhombus Transformation and Digital Tube Model," *Entropy*, vol. 27, no. 8, pp. 1–32, Aug. 2025, doi: 10.3390/e27080874.