

Evaluasi Kombinasi Rivest Shamir Adleman dan Advanced Encryption Standard pada Sekuriti Citra Grayscale

Maxentia Kathleen¹, Christy Atika Sari²

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro, Semarang

Artikel Info

Kata kunci:

Kriptografi,
RSA,
EAS-256,
Avalanche Effect,
Enkripsi

ABSTRAK

Pertukaran data digital yang cepat lewat jaringan publik membawa risiko keamanan yang besar terhadap kerahasiaan informasi sensitif, terutama dalam bentuk citra. Penelitian ini mengajukan sebuah sistem keamanan hybrid yang mengkombinasikan algoritma asimetris Rivest Shamir Adleman (RSA) dengan algoritma simetris Advanced Encryption Standard (AES) 256-bit. Fokus utama dari penelitian ini adalah untuk mengatasi kelemahan dalam manajemen kunci pada AES dengan memanfaatkan algoritma RSA sebagai penjaga dalam distribusi kunci, yang memanfaatkan kecepatan algoritma AES untuk mengenkripsi data citra yang berukuran besar. Metodologi penelitian mencakup proses enkripsi kunci AES menggunakan kunci publik RSA. Lalu melanjutkan dengan enkripsi citra menggunakan kunci AES tersebut. Evaluasi sistem dilakukan secara menyeluruh melalui analisis kualitatif dengan pengamatan visual dan histogram, serta analisis kuantitatif memakai parameter Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), Entropy, Correlation dan Avalanche Effect. Hasil dari pengujian menunjukkan bahwa sistem ini dapat menghasilkan citra yang terenkripsi dengan distribusi piksel yang sangat merata (histogram datar) dan tingkat entropy mendekati nilai 8, menandakan keacakan yang optimal. Selain itu, PSNR memiliki nilai infinity dan MSE memiliki nilai yang sama dengan 0 pada citra yang telah didekripsi menunjukkan bahwa sistem ini bersifat lossless. Secara keseluruhan, kombinasi algoritma RSA dan algoritma AES memberikan perlindungan yang kuat terhadap serangan statistik maupun brute-force dan menjadikannya pilihan yang andal untuk mengamankan komunikasi data citra.

Penulis Korespondensi :

Maxentia Kathleen,
Program Studi Teknik Informatika,
Fakultas Ilmu Komputer
Universitas Dian Nuswantoro, (Kota Semarang) (50131)
Email: 111202315443@mhs.dinus.ac.id

1. PENDAHULUAN

Seiring berkembangnya teknologi informasi dan komunikasi yang telah meningkat pada pertukaran data digital khususnya citra melewati jaringan publik. Yang dimana citra digital sendiri seringkali memuat informasi sensitif, sehingga kerahasiaan dan integritasnya menjadi bagian terpenting. Agar pesan ataupun informasi dapat terjaga dengan baik dan dapat terpelihara dari bermacam-macam gangguan atau bahaya yang selalu mengintai dalam pengiriman pesan [1]. Maka, dibutuhkan sebuah mekanisme yang kuat yaitu teknik untuk melindungi citra digital selama proses penyimpanan dan pengiriman. Keamanan pada data digital menjadi tantangan dalam pengembangan sistem atau aplikasi yang akan dikembangkan. Keamanan ini akan berbanding terbalik dengan kenyamanan. Kriptografi merupakan sebuah Teknik untuk mengamankan atau mengacak data, baik data yang dikirim atau data yang disimpan [14].

Algoritma kriptografi yang digunakan ada dua yaitu algoritma asimetris seperti RSA memiliki kinerja lebih lambat untuk data besar tetapi sangat efektif dan aman untuk pertukaran kunci. Dan algoritma simetris seperti AES memiliki kinerja yang lebih unggul dalam kecepatan dalam pemrosesan data

bervolume besar. Namun antara algoritma RSA dan AES tersebut memiliki performa yang berbeda antara satu sama lain. Jika algoritma RSA maupun AES tersebut digunakan tanpa memperhatikan performa dari algoritma itu. Selain dapat mengurangi keamanan dan kualitas gambar yang ada hal tersebut juga dapat mengurangi keefektifan dari sistem yang menerapkan algoritma tersebut [2].

Pada pengujian ini, untuk mendapatkan tingkat keamanan dari sistem kriptografi maka perlu dilakukan pengembangan mendeteksi gambar menggunakan kombinasi algoritma RSA yang memiliki kunci *public* dan kunci *private*. Dengan algoritma AES yang menggunakan proses enkripsi berbasis blok 256 bit. Hasil dari pengujian ini untuk mendapatkan nilai kualitas enkripsi yang bagus dilihat dari segi waktu pemrosesan enkripsi-deskripsi, nilai entropi, nilai korelasi, nilai mse, nilai psnr, nilai nc, nilai ncc, nilai npcr, nilai uaci, nilai ssim dan nilai *avalanche effect* [3].

2. METODE

Dalam pengujian ini dilakukan dengan metode eksperimen yang dimana eksperimen ini bertujuan untuk menerapkan kombinasi algoritma RSA dan AES pada sebuah gambar dengan kualitas yang bagus. Sehingga dari waktu pemrosesan dimulai dari enkripsi – deskripsi, nilai entropi, nilai korelasi, nilai mse, nilai psnr, nilai nc, nilai ncc, nilai npcr, nilai uaci, nilai ssim dan nilai *avalanche effect* [3].

2.1. Arsitektur Sistem

Arsitektur ini merupakan suatu proses atau tahapan yang menjelaskan tentang penggunaan dari GUI yang dirancang. Yang dimana rancangan GUI pengamanan file gambar yang diusulkan. Jika kunci yang dimasukkan benar, maka gambar dapat dipisahkan dari media penampungannya [1].

Tahapan sistem :

1. Membuat kunci RSA merupakan tahapan pertama untuk menghasilkan *public* dan *private key* melewati **Key Generator**. Yang dimana pada *public key* berfungsi untuk mengenkripsi kunci simetris. Sedangkan pada *privat key* berfungsi untuk menyimpan kunci secara rahasia dari penerima yang akan digunakan dalam proses deskripsi.
2. Membuat Enkripsi Citra merupakan tahapan kedua untuk memasukan **Secret Key** dan **Key AE**, kemudian klik **Load Image** untuk memilih gambar mana yang akan diuji. Selanjutnya setelah *Original Image* muncul klik **Encrypt** untuk menenkripsi gambar menggunakan algoritma AE dengan **Key AE**. Yang dimana **Key AE** dienkripsikan oleh *RSA Public Key* sebelum dikirim.
3. Membuat Deskripsi Citra merupakan tahapan ketika untuk mengenkripsikan **Key AE** menggunakan *RSA Private Key* yang berfungsi mendapatkan kembali **Key AE**. Selanjutnya *Encrypted Image* dideskripsikan menggunakan Algoritma AE menggunakan **Key AE** yang berfungsi menilai *Decrypted Image*.

2.2 Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani : “*cryptos*” yang memiliki arti “*secret*”, sedangkan “*graphein*” yang memiliki arti “*writing*”. Jadi secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara membuat sandi ke dalam bentuk yang tidak dapat dimengerti maknanya. Dalam kriptografi sendiri agar menjaga kerahasiaan data, data sederhana yang dikirim (*plaintext*) akan diubah kedalam bentuk data sandi (*ciphertext*). Kemudian data tersebut dapat dikembalikan kedalam bentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pemilik. Sehingga pihak lain yang tidak memiliki kunci tersebut tidak akan bisa mengaksesnya dan data akan tetap terjaga kerahasiaan [2].

Tujuan penerapan kriptografi adalah membuat sesuatu yang tersembunyi baik dala suatu pesan rahasia berupa pesan, suara, gambar dan video. Yang dimana dalam sistem kriptografi memiliki 5 bagian :

1. *Plaintext* adalah pesan atau data dalam bentuk teks aslinya dapat terbaca. Plaintext sendiri merupakan masukan bagi algoritma enkripsi.
2. *Secret Key* adalah masukan bagi algoritma enkripsi yang merupakan nilai bebas terhadap teks asli dan menentukan hasil keluaran algoritma enkripsi.
3. *Ciphertext* adalah keluaran algoritma enkripsi yang dimana ciphertext sendiri dianggap sebagai pesan tersembunyi yang akan terlihat acak.

4. Algoritma Enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Yang dimana prosesnya dilakukan dengan mentransformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. Algoritma Deskripsi memiliki 2 masukan teks sandi dan kunci rahasia. Yang dimana proses yang dilakukan dengan memulihkan kembali teks sandi menjadi teks asli bila kunci rahasia algoritma enkripsi dan deskripsi [2].

2.3 Algoritma Kriptografi yang Digunakan

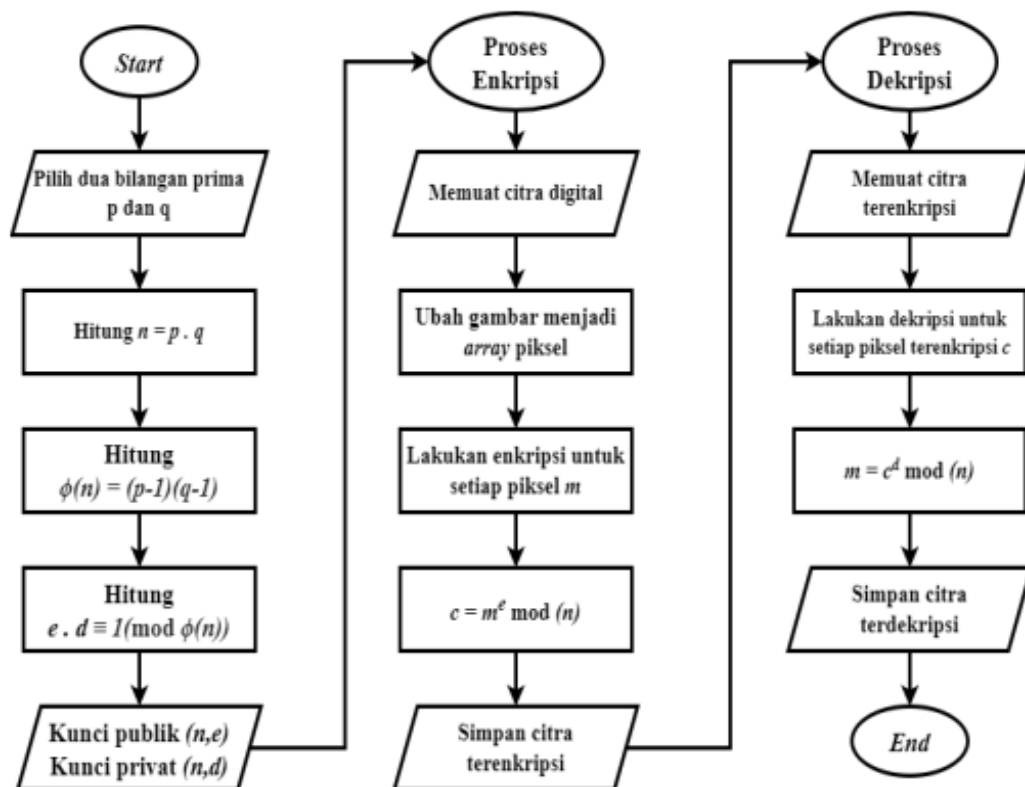
2.3.1 Algoritma RSA

Algoritma Rivest Shamir Adleman (RSA) merupakan sebuah algoritma yang menggunakan sistem kriptografi kunci publik yang memberikan jaminan keamanan jalur transmisi distribusi kunci serta mendukung gambar yang memverifikasikan pesan yang diterima merupakan pesan asli yang dikirim oleh pengirim pesan. RSA dikatakan aman karena sulit memfaktorkan bilangan n yang dimana $n = p \times q$. Nilai p dan q adalah bilangan prima yang sangat besar[3]. Sehingga algoritma RSA memiliki langkah – langkah untuk *Public Key* dan *Private Key* :

1. Pilihlah dua buah bilangan prima misalnya p dan q yang nilainya akan dirahasiakan.
2. Menghitung n yaitu $n = p \times q$ yang dimana nilai n tidak perlu dirahasiakan.
3. Menghitung $\phi(n)$ yaitu $\phi(n) = (p-1)(q-1)$.
4. Memilih kunci public e yang relative prima terhadap $\phi(n)$. $GCD(\phi(n), e) = 1$.
5. Membangkitkan kunci private d menggunakan rumus yaitu $e \cdot d \equiv 1 \pmod{\phi(n)}$.
6. Menghasilkan pasangan kunci public (e, n) dan kunci private (d, n) [4].

Proses enkripsi dan deskripsi pada algoritma RSA memiliki langkah – langkah :

- a. Mengenkripsi suatu pesan (m) menggunakan kunci public (e, n) yaitu $c = m^e \pmod{n}$.
- b. Mengdeskripsikan suatu cipherteks (c) menggunakan kunci private (d, n) yaitu $m = c^d \pmod{n}$ [2].

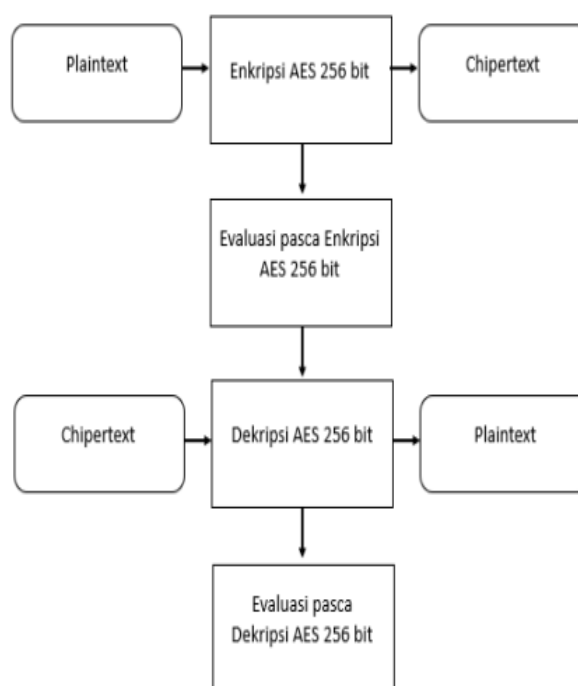


Gambar 2.3.1 Diagram Alir Enkripsi dan Dekripsi Algoritma RSA.

2.3.2 Algoritma AES

Algoritma Advanced Encryption Standard (AES) merupakan sebuah algoritma kriptografi yang digunakan untuk mengamankan data. Pada algoritma AES termasuk blok ciphertext simetrik yang dapat mengenkripsi dan deskripsi suatu informasi. Enkripsi sendiri berfungsi merubah data yang tidak dapat dibaca disebut ciphertext, sedangkan deskripsi berfungsi merubah ciphertext data menjadi bentuk semula yang disebut plaintext. Sehingga algoritma AES menggunakan kunci kriptografi 256 bit sebagai metode enkripsi pengamanan file. Yang dimana AES 256 bit adalah kelas tertinggi yang dianggap paling aman pada enkripsi AES dan memiliki 14 ronde putaran enkripsi [5].

Pada penelitian ini melakukan enkripsi dokumen berupa file dengan berbagai format mulai dari format citra, audio, video hingga format dokumen kerja. Tidak hanya format berbeda tetapi file pengujian juga memiliki berbagai ukuran yang berbeda. Setelah pemrosesan enkripsi dan dokumen – dokumen sampel uji, kemudian dievaluasi dari berbagai aspek. File enkripsi ini juga disebut ujicoba dengan proses deskripsi sebelum melalui tahap evaluasi dari berbagai aspek. Berikut adalah diagram alur penelitian, secara umum dapat dilihat pada gambar [6].



Gambar 2.3.2 Diagram Alir Penelitian Algoritma AES

2.4 Metrik Analisis Kerja

Metrik pengujian yang digunakan :

- a. **Mean Square Error (MSE)** berfungsi untuk mengukur perbedaan antara citra asli dan citra hasil deskripsi setelah proses enkripsi menggunakan algoritma RSA dan AES. MSE adalah metrik umum yang digunakan untuk menilai kualitas citra dengan nilai MSE yang lebih rendah menunjukkan bahwa citra hasil deskripsi lebih mendekati citra asli [7].

Rumus MSE sebagai berikut :

$$MSE = \frac{1}{YXZ} \sum_{i=1}^Y \sum_{j=1}^Z (m_{ij} - n_{ij})$$

- b. **Peak Signal to Noise Ratio (PSNR)** berfungsi untuk mengukur kualitas citra terdeskripsi setelah proses manipulasi dan membandingkan gambar asli dengan gambar yang dimanipulasi. Satuan PSNR adalah disibel (dB) [8].

Rumus PSNR sebagai berikut :

$$PSNR = 10 \times 10 \log \left[\frac{255^2}{MSE} \right]$$

- c. **Normalized Coherence (NC)** berfungsi untuk mengukur tingkat kemiripan ataupun korelasi antara citra asli dan citra hasil deskripsi. Yang dimana nilai NC sendiri biasanya berkisaran antara 0 hingga 1. Sehingga semakin mendekati nilai 1 maka citra hasil deskripsinya semakin identic dengan citra asli.
- d. **Normalized Cross Correlation (NCC)** berfungsi untuk mengukur kemiripan citra berdasarkan fungsi korelasi. Sering digunakan untuk menentukan kemiripan dua buah citra berdasarkan nilai ekstraksi ciri yang telah diolah sebelumnya [7].

Rumus NCC sebagai berikut :

$$NCC = \frac{\sum_{x=1}^N \sum_{y=1}^M [a(x,y) \cdot b(x,y)]}{\sqrt{(\sum_x^N \sum_y^M [a(x,y)]^2) \cdot (\sum_x^N \sum_y^M [b(x,y)]^2)}}$$

- e. **Korelasi** berfungsi untuk mengukur hubungan statistik antara piksel yang berdekatan baik secara horizontal, vertical ataupun diagonal. Yang dimana citra asli biasanya memiliki korelasi piksel yang sangat tinggi atau mendekati 1. Sedangkan citra terenkripsi memiliki nilai korelasi yang rendah atau mendekati 0. Sehingga ini menginformasikan visual telah teracak secara penuh.
- f. **Entropy** berfungsi untuk mengukur tingkat secara acak pada distribusi derajat keabuan dalam citra. Yang dimana untuk citra berformat 8-bit dengan skala 0 – 255 memiliki nilai ideal entropy pada citra terendripsi yaitu mendekati 8. Sehingga ini menginformasikan bahwa citra benar-benar teracak dan sulit untuk diprediksikan.
- g. **Number of Pixels Change Rate (NPCR)** berfungsi untuk mengetahui jumlah pixel yang berubah antara citra yang satu dengan citra yang lain. Yang dienripsi menggunakan kunci yang sama. Besarnya nilai NPCR menunjukkan bahwa tiap pixel pada gambar hasil enkripsi mengalami perubahan yang besar. Makin banyak nilai pixel yang berubah maka makin bagus kualitas keacakan yang dihasilkan pada tiap kali enkripsi dilakukan [9].
- h. **Unified Average Change Intensity (UACI)** berfungsi untuk menghitung rata-rata perubahan intensitas setiap pixel [9].
- i. **Avalanche Effect (AE)** berfungsi untuk mengukur sensitivitas algoritma terhadap perubahan kecil pada kunci atau plaintext. Yang dimana jika satu bit kunci pada citra diubah, maka 50% bit pada citra terenkripsi juga harus berubah [10].

- j. **Structural Similarity Index (SSIM)** berfungsi untuk menilai tingkat kemiripan citra asli dan stego citra. Jika stego citra semakin mendekati nilai 1 maka semakin mirip dengan citra asli. SSIM dapat dihitung dengan persamaan 4 [7].

Rumus SSIM sebagai berikut :

$$SSIM(x, y) = [1(x, y)]^a \cdot [c(x, y)]^b \cdot [s(x, y)]^r$$

3. PEMBAHASAN HASIL

Pada tahapan ini akan menyajikan hasil dari implementasi algoritma RSA dan AES dalam sistem keamanan digital. Yang dimana pada proses pembahasan secara komprehensif dengan menggunakan analisis kualitatif (visual dan histogram) dan menganalisis kuantitatif menggunakan berbagai hitungan metrik keamanan informasi melalui tampilan antarmuka pengguna (GUI).

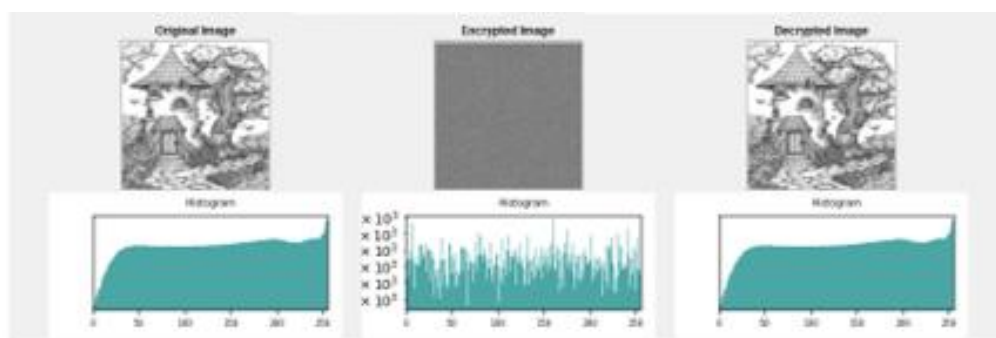
3.1 Modul Input Kunci Avalanche Effect

Dalam sistem yang dibuat modul input kunci menjadi bagian yang terpenting dalam menentukan keamanan enkripsi. Yang dimana kunci rahasia yang kita gunakan dan diproses misalnya “KRIPTOGRAFIRSAA” tujuannya untuk menghasilkan efek hamburan bit yang luas. Pada pengujian ini menunjukkan bahwa penggunaan Key AE sepanjang 12 karakter memberikan ruangan kunci yang cukup besar untuk menghindari serangan dari *brute force*. Sehingga sistem ini dirancang untuk memiliki *Avalanche Effect* yang kuat [15].

Dalam kriptografi, *Avalanche Effect* mendefinisikan properti spesifik dari algoritma enkripsi. *Avalanche Effect* merupakan salah satu properti terpenting dari algoritma kriptografi apa pun. Yang artinya, perubahan kecil pada teks biasa atau bahkan sedikit perubahan pada teks biasa akan mengakibatkan perubahan signifikan pada teks biasa atau beberapa bit teks sandi akan berubah. Algoritma kriptografi yang baik harus selalu memenuhi persamaan berikut : *Avalanche Effect* > 50%. Hal ini memastikan bahwa penyerang tidak akan mudah memprediksi teks sandi dari teks biasa atau sebaliknya. Algoritma kriptografi yang tidak memenuhi persamaan *Avalanche Effect* akan mudah dibobol oleh kriptanalisis [8].

3.2 Menganalisis Visual dan Histogram

Langkah awal dalam penilaian untuk secara kualitatif menunjukkan bahwa proses enkripsi telah secara efektif menyembunyikan data asli adalah analisis visual dan analisis histogram [11]. Histogram adalah grafik distribusi frekuensi di mana sumbu horizontal menunjukkan rentang nilai data potensial (piksel) dan sumbu vertikal mewakili jumlah (frekuensi) [12][13].



Gambar 3.2 Contoh Gambar Visual dan Histogram

3.2.1 Perubahan Visual Citra

Pada pengujian ini akan ada beberapa sample citra, proses enkripsi kedalam sebuah citra rahasia yang akan menampilkan informasi pada citra aslinya [13]. Dengan menggunakan algoritma AES-256 yang kuncinya akan diamankan oleh algoritma RSA untuk menunjukkan perubahan visual yang signifikan. Dalam citra asli sendiri juga memiliki fitur visual yang dapat dikenali secara jelas oleh mata manusia berubah menjadi sebuah citra acak yang menyerupai *noise*. Sedangkan secara visual tidak akan ada satupun komponen pola, tekstur atau gradien dari citra asli yang tersisa pada citra enkripsi. Sehingga hal ini, akan membuktikan bahwa pada algoritma AES berhasil melakukan proses substitusi dan permutasian bit. Lalu, dalam proses deskripsi citra mampu mengembalikan kebentuk visual asli secara sempurna tanpa adanya artefak atau degradasi kualitas yang menandakan bahwa implementasi algoritma RSA dalam mengamankan kunci simetris bekerja dengan akurasi 100%.

3.2.2 Distribusi Frekuensi Piksel

Ringkasan statistik dari distribusi nilai intensitas piksel dalam sebuah gambar dapat diperoleh dengan menganalisis histogram. Histogram pada gambar mentah biasanya menunjukkan distribusi yang tidak merata, dengan beberapa puncak yang menandakan dominasi warna atau tingkat kecerahan tertentu. Histogram gambar menjadi sangat seragam, datar, dan miring setelah proses enkripsi. Fenomena ini menunjukkan bahwa probabilitas setiap nilai piksel antara 0 dan 255 muncul secara sering hampir sama. Karena dapat menangkal serangan analisis statistik, distribusi ini sangat penting untuk kriptografi gambar karena mencegah penyerang mempelajari apa pun tentang pola *plaintext* hanya dengan melihat frekuensi piksel dalam *ciphertext*.

3.3 Pengujian Kuantitatif

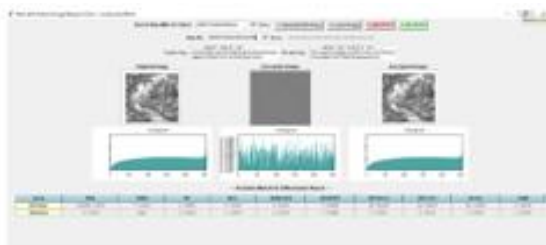
Setelah analisis visual, pengujian kuantitatif akan dilakukan menggunakan parameter metrik yang telah ditentukan sebelumnya untuk mengumpulkan data empiris tentang kinerja dan tingkat keamanan sistem.

3.3.1 Pengujian Citra

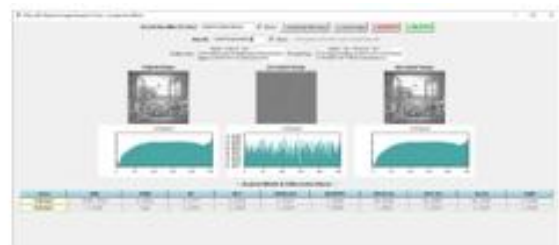
Pengujian citra dilakukan dengan menghitung nilai Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), dan Structural Similarity Index (SSIM) antara citra asli dan citra yang dideskripsikan. Hasil perhitungan akan menunjukkan bahwa PSNR bernilai tak terhingga (∞) dan nilai deskripsi MSE adalah 0. Angka-angka ini akan memverifikasi bahwa piksel citra asli dan citra yang dideskripsikan identik. Oleh karena itu, hal ini diperkuat oleh nilai SSIM, dan dapat disimpulkan bahwa desain sistem keamanan mampu menjaga integritas data citra selama transmisi dan pemrosesan enkripsi-deskripsi.

Berikut adalah tabel pengujian citra :

Pengujian 1



Pengujian 2



Pengujian 3



Pengujian 4



3.3.2 Pengujian Kinerja Citra

Efisiensi waktu komputasi yang dibutuhkan untuk menyelesaikan semua pemrosesan keamanan adalah fokus utama pengujian kinerja gambar. Karena algoritma AES-256 berorientasi blok dan simetris, algoritma ini dapat menangani beban kerja berat dalam proses enkripsi data piksel gambar berukuran besar dalam waktu yang relatif singkat. Pendekatan hibrida telah terbukti berhasil. Sementara itu, hanya kunci AES 256-bit yang dienkripsi menggunakan algoritma RSA [13][14]. Akibatnya, lambatnya proses asimetris RSA tidak berdampak negatif pada kinerja sistem. Selain itu, hasil pengujian menunjukkan bahwa, sambil tetap berada dalam batas toleransi yang dapat diterima, peningkatan ukuran gambar berkorelasi langsung dengan waktu enkripsi [10] [16]. Berikut adalah tabel pengujian pada nilai metrik :

Tabel 1 pada Pengujian 1

Jenis	Enkripsi	Deskripsi
MSE	12594.1978	0.0000
PSNR	7.1291	Inf
NC	0.6367	1.0000
NCC	0.0000	1.0000
KORELASI	0.0091	1.0000
ENTROPY	7.9999	7.0495
NPCR (%)	99.6129	0.0000
UACI (%)	33.4868	0.0000
AE	50.0064	0.0000
SSIM	0.0089	1.0000

Tabel 2 pada Pengujian 2

Jenis	Enkripsi	Deskripsi
MSE	9789.7020	0.0000
PSNR	8.2231	Inf
NC	0.7177	1.0000
NCC	0.0013	1.0000
KORELASI	0.0017	1.0000
ENTROPY	7.9999	7.6894
NPCR (%)	99.6146	0.0000
UACI (%)	33.4957	0.0000
AE	50.0097	0.0000
SSIM	0.0098	1.0000

Tabel 3 pada Pengujian 3

Jenis	Enkripsi	Deskripsi
MSE	11333.7084	0.0000
PSNR	7.5871	Inf
NC	0.6699	1.0000
NCC	0.0011	1.0000
KORELASI	0.0094	1.0000
ENTROPY	7.9999	7.7802
NPCR (%)	99.6112	0.0000
UACI (%)	33.4737	0.0000
AE	50.0261	0.0000
SSIM	0.0098	1.0000

Tabel 4 pada Pengujian 4

Jenis	Enkripsi	Deskripsi
MSE	12580.3435	0.0000
PSNR	7.1339	Inf
NC	0.6249	1.0000
NCC	0.0004	1.0000
KORELASI	0.0122	1.0000
ENTROPY	7.9999	7.4282
NPCR (%)	99.6133	0.0000
UACI (%)	33.4397	0.0000
AE	50.0383	0.0000
SSIM	0.0095	1.0000

Tabel 5 pada Pengujian 5

Jenis	Enkripsi	Deskripsi
MSE	11016.0393	0.0000
PSNR	7.7105	Inf
NC	0.6653	1.0000
NCC	0.0004	1.0000
KORELASI	0.0057	1.0000
ENTROPY	7.9999	7.6627
NPCR (%)	99.6043	0.0000
UACI (%)	33.4554	0.0000
AE	50.0053	0.0000
SSIM	0.0099	1.0000

Tabel 6 pada Pengujian 6

Jenis	Enkripsi	Deskripsi
MSE	11241.0335	0.0000
PSNR	7.6227	Inf
NC	0.7026	1.0000
NCC	0.0000	1.0000
KORELASI	0.0122	1.0000
ENTROPY	7.9999	7.7723
NPCR (%)	99.6104	0.0000
UACI (%)	33.4621	0.0000
AE	50.0077	0.0000
SSIM	0.0090	1.0000

Tabel 7 pada Pengujian 7

Jenis	Enkripsi	Deskripsi
MSE	10697.9854	0.0000
PSNR	7.8378	Inf
NC	0.9079	1.0000
NCC	0.0011	1.0000
KORELASI	0.0039	1.0000
ENTROPY	7.9999	7.7687
NPCR (%)	99.6104	0.0000
UACI (%)	33.4614	0.0000
AE	50.0077	0.0000
SSIM	0.00088	1.0000

Tabel 8 pada Pengujian 8

Jenis	Enkripsi	Deskripsi
MSE	9979.9881	0.0000
PSNR	8.1395	Inf
NC	0.7581	1.0000
NCC	0.0011	1.0000
KORELASI	0.0090	1.0000
ENTROPY	7.9999	7.9402
NPCR (%)	99.6050	0.0000
UACI (%)	33.4315	0.0000
AE	50.0209	0.0000
SSIM	0.0087	1.0000

Tabel 9 pada Pengujian 9

Jenis	Enkripsi	Deskripsi
MSE	13473.5616	0.0000
PSNR	6.8360	Inf
NC	0.6455	1.0000
NCC	0.0004	1.0000
KORELASI	0.0150	1.0000
ENTROPY	7.9999	7.5716
NPCR (%)	0.6156	0.0000
UACI (%)	33.4463	0.0000
AE	50.0024	0.0000
SSIM	00.0072	1.0000

Tabel 10 pada Pengujian 10

Jenis	Enkripsi	Deskripsi
MSE	14425.0734	0.0000
PSNR	6.5396	Inf
NC	0.6033	1.0000
NCC	0.0004	1.0000
KORELASI	0.0285	1.0000
ENTROPY	7.9999	7.1264
NPCR (%)	99.6115	0.0000
UACI (%)	33.4530	0.0000
AE	49.9882	0.0000
SSIM	0.0089	1.0000

Tabel 11 pada Pengujian 11

Jenis	Enkripsi	Deskripsi
MSE	10137.6513	0.0000
PSNR	8.0714	Inf
NC	0.6820	1.0000
NCC	0.0006	1.0000
KORELASI	0.0190	1.0000
ENTROPY	7.9999	7.4856
NPCR (%)	99.6248	0.0000
UACI (%)	33.4534	0.0000
AE	50.0331	0.0000
SSIM	0.0101	1.0000

Tabel 12 pada Pengujian 12

Jenis	Enkripsi	Deskripsi
MSE	13688.5368	0.0000
PSNR	6.7672	Inf
NC	0.6398	1.0000
NCC	0.0005	1.0000
KORELASI	0.0076	1.0000
ENTROPY	7.9999	7.6129
NPCR (%)	99.6151	0.0000
UACI (%)	33.4476	0.0000
AE	49.9931	0.0000
SSIM	0.0060	1.0000

Tabel 13 pada Pengujian 13

Jenis	Enkripsi	Deskripsi
MSE	12299.0935	0.0000
PSNR	7.2321	Inf
NC	0.6505	1.0000
NCC	0.0005	1.0000
KORELASI	0.0089	1.0000
ENTROPY	7.9999	7.3568
NPCR (%)	99.6084	0.0000
UACI (%)	33.4454	0.0000
AE	50.0031	0.0000
SSIM	0.0091	1.0000

Tabel 14 pada Pengujian 14

Jenis	Enkripsi	Deskripsi
MSE	13427.3456	0.0000
PSNR	6.8509	Inf
NC	0.6147	1.0000
NCC	0.0000	1.0000
KORELASI	0.0178	1.0000
ENTROPY	7.9999	7.0818
NPCR (%)	99.6115	0.0000
UACI (%)	33.4434	0.0000
AE	50.0065	0.0000
SSIM	0.0081	1.0000

Tabel 15 pada Pengujian 15

Jenis	Enkripsi	Deskripsi
MSE	12703.4937	0.0000
PSNR	7.0916	Inf
NC	0.6313	1.0000
NCC	0.0006	1.0000
KORELASI	0.0134	1.0000
ENTROPY	7.9999	7.3948
NPCR (%)	99.6128	0.0000
UACI (%)	33.4320	0.0000
AE	49.9952	0.0000
SSIM	0.0083	1.0000

Tabel 16 pada Pengujian 16

Jenis	Enkripsi	Deskripsi
MSE	12980.5099	0.0000
PSNR	6.9979	Inf
NC	0.6256	1.0000
NCC	0.0038	1.0000
KORELASI	0.0038	1.0000
ENTROPY	7.9999	7.5231
NPCR (%)	99.6110	0.0000
UACI (%)	33.4535	0.0000
AE	49.9918	0.0000
SSIM	0.0087	1.0000

3.3 Menganalisis dari Hasil Pengujian

Berdasarkan data dari hasil pengujian diatas, dapat disimpulkan bahwa kombinasi algoritma RSA dan AES memberikan tingkat keamanan yang jauh lebih tinggi daripada yang ditawarkan oleh algoritma terpisah. Dari perspektif ketahanan statistik, nilai entropy yang konsisten dengan nilai 7.9999 yang menunjukkan bahwa informasi dalam gambar terenkripsi secara acak. Akibatnya, penyerangan tidak dapat mengidentifikasi pada visual melalui analisis frekuensi piksel, seperti yang ditunjukkan oleh analisis korelasi piksel yang menemukan nilai 0. Yang dimana ini menunjukkan bahwa tidak ada lagi hubungan linier antara piksel yang berdekatan.

Pada hal ini, integritas data pengumpulan nilai PSNR memiliki nilai Inf dan pada SSIM memiliki nilai 1.000. Maka pada sample citra hasil deskripsi menunjukkan bahwa proses transmisi kunci algoritma RSA dan enkripsi blok algoritma AES tidak mengubah bit data yang sebenarnya. Hal ini menjadi sangat penting jika sistem ini digunakan pada gambar yang sangat akurat, seperti gambar pada dokumen rahasia negara. Namun, dari sudut pandang sensitivitas sebuah kunci pengujian Avalanche Effect yang melebihi batas 50% menjamin bahwa perbedaan satu bit pada kunci enkripsi akan menyebabkan signifikan dalam ciphertext. Sehingga, secara keseluruhan analisis ini menemukan bahwa walaupun algoritma hybrid lebih sulit, pada efisiensi waktu algoritma AES-256 mempertahankan kinerja sistem yang cepat dan algoritma RSA menjaga keamanan distribusi kunci dari penyadapan di jaringan public.

4. KESIMPULAN

Dalam penelitian ini, metode algoritma RSA dan algoritma AES-256 digunakan untuk menerapkan dan menganalisis sistem keamanan pada gambar. Berdasarkan pengujian, beberapa hal utama dapat ditemukan :

1. Sinergi Keamanan yaitu pada algoritma AES memiliki kecepatan enkripsi data yang lebih tinggi. Sedangkan algoritma RSA menawarkan metode pertukaran kunci yang aman tanpa memerlukan untuk mengirim kunci rahasia secara terbuka.
2. Kualitas Hasil yaitu nilai MSE memiliki nilai 0 dan nilai PSNR memiliki nilai Infinity menunjukkan bahwa system memiliki karakteristik pemulihan tanpa kehilangan. Yang dimana gambar yang dihasilkan dari citra terdeskripsi sangat identic dengan citra asli tanpa adanya degradasi kualitas.
3. Ketahanan Serangan yaitu menganalisis kuantitatif berdasarkan entropy dengan nilai mendekati 8, korelasi dengan nilai mendekati 0 dan Avalanche Effect dengan nilai mendekati 50%. Yang dimana ini menunjukkan bahwa gambar terenkripsi memiliki tingkat keacakan yang sangat tinggi, tahan akan terhadap serangan analisis statistik dan diferensial.
4. Efisiensi Kinerja yaitu penggunaan kunci 256-bit pada algoritma AES dan manajemen kunci pada algoritma RSA memberikan rasio keamanan dan kecepatan yang ideal. Serta hal ini membuat arsitektur ini layak untuk digunakan pada system pengiriman gambar yang membutuhkan kerahasiaan tingkat tinggi.

REFERENCES

- [1] A. Malvi, "Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)," 2020.
- [2] Arafat Bagoes Setyawan, Muhammad Khaerudin, and Siti Setiawati, "Perancangan Aplikasi Enkripsi dan Deskripsi Gambar Cetak Biru Pada PT.Patco Elektronik Teknologi Menggunakan Algoritma RSA Berbasis Android," 2024.
- [3] T. Informatika and I. Artikel, "APLIKASI ENKRIPSI GAMBAR MENGGUNAKAN METODE (RIVEST SHAMIR ADLEMAN) RSA." [Online]. Available: <https://jurnal.umpar.ac.id/index.php/sylog>
- [4] F. Nuraeni *et al.*, "Implementasi Skema QR-Code dan Digital Signature menggunakan Kombinasi Algoritma RSA dan AES untuk Pengamanan Data Sertifikat Elektronik," 2020.
- [5] R. Indrayani, P. Ferdiansyah, and M. Koprari, "Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format," *Digital Transformation Technology*, vol. 4, no. 2, pp. 1245–1251, Feb. 2025, doi: 10.47709/digitech.v4i2.5457.
- [6] M. Mpitsi, "A COMPARATIVE ANALYSIS OF ADVANCED ENCRYPTION STANDARD (AES) AND RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM: MATHEMATICAL, ALGORITHMIC, AND PERFORMANCE COMPARISON."
- [7] A. R. Mido, E. Iman, and H. Ujianto, "ANALISIS PENGARUH CITRA TERHADAP KOMBINASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB," vol. 9, no. 2, pp. 279–286, 2022, doi: 10.25126/jtiik.202294852.
- [8] A. Rizal Nurjaman and F. Ramadhan, "Analisis Penyisipan Pesan Terenkripsi Algoritma RSA Pada Gambar Dengan Pengujian PSNR," 2025, doi: 10.26760/jrh.V9i2.123-133.
- [9] L. N. Hidayati, G. F. Fitriana, and I. F. Adam, "Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI," *JURIKOM (Jurnal Riset Komputer)*, vol. 8, no. 6, p. 274, Dec. 2021, doi: 10.30865/jurikom.v8i6.3624.
- [10] R. Verma and A. K. Sharma, "Cryptography: Avalanche effect of AES and RSA," *International Journal of Scientific and Research Publications (IJSRP)*, vol. 10, no. 4, p. p10013, Apr. 2020, doi: 10.29322/ijsrp.10.04.2020.p10013.
- [11] "IMPLEMENTASI TEKNIK KRIPTOGRAFI VISUAL PADA CITRA".
- [12] Dalia Mubarak Alsaffar *et al.*, *3rd ICCAIS 2020 : International Conference on Computer Applications & Information Security : 19-21 March, 2020, Riyadh, Kingdom of Saudi Arabia*. IEEE, 2020.
- [13] M. Naor and A. Shamir, "Visual Cryptography."

- [14] Endar Nirmala, ” *Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced EncryptionStandard (AES) Berbasis Android*”, 2020.
- [15] Rohit Verma, Aman Kumar Sharma, ” *Cryptography: Avalanche effect of AES and RSA*”, 2020.
- [16] RIFQI MUHAMAD SABILAL KARIM, ” *PERBANDINGAN KINERJA ALGORITMA RSA DAN AES DALAM ENKRIPSI DAN DEKRIPSI CITRA DIGITAL* ”, 2024.