

Studi Komparatif Algoritma RSA dan AES pada Enkripsi dan Dekripsi Citra Digital

Rifqi Muhamad Sabilal Karim*, Muhammad Khudzaifah, Fachrur Rozi

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

19610111@student.uin-malang.ac.id*, khudzaifah@uin-malang.ac.id, f.rozi@mat.uin-malang.ac.id

Abstrak

Di era digital, perlindungan data menjadi prioritas, terutama untuk citra digital yang bernilai penting di bidang komunikasi, keamanan, dan medis. Penelitian ini membandingkan kinerja algoritma RSA dan AES dalam enkripsi dan dekripsi citra digital, menggunakan tiga parameter utama: waktu proses, perubahan ukuran file, dan kualitas citra yang diukur dengan *Mean Squared Error* (MSE). Studi ini dilakukan secara kuantitatif eksperimental pada 50 citra digital beresolusi kecil dan sedang. RSA menggunakan kunci publik dan privat, sedangkan AES memanfaatkan proses *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey*. Hasil menunjukkan AES lebih cepat dalam enkripsi dan dekripsi dibandingkan RSA. Namun, kualitas citra hasil enkripsi RSA lebih rendah, sebagaimana terlihat dari nilai MSE yang lebih tinggi. Dari segi ukuran file, RSA cenderung menghasilkan file lebih kecil, sementara AES menghasilkan ukuran yang lebih besar. Penelitian ini memberikan panduan bagi pemilihan algoritma enkripsi yang sesuai dengan kebutuhan aplikasi tertentu, khususnya dalam keamanan data visual. Temuan ini diharapkan membantu mahasiswa dan praktisi keamanan informasi dalam menentukan algoritma optimal untuk melindungi citra digital dari ancaman.

Kata kunci: Citra Digital; RSA; AES; MSE; Keamanan Data

Abstract

In the digital era, data protection has become a priority, especially for digital images that hold significant value in the fields of communication, security, and medicine. This study compares the performance of the RSA and AES algorithms in encrypting and decrypting digital images, using three main parameters: processing time, file size change, and image quality measured by Mean Squared Error (MSE). This study was conducted experimentally in a quantitative manner on 50 digital images of small and medium resolution. RSA uses public and private keys, while AES utilizes the *SubBytes*, *ShiftRows*, *MixColumns*, and *AddRoundKey* processes. The results show that AES is faster in encryption and decryption compared to RSA. However, the quality of the image resulting from RSA encryption is lower, as evidenced by the higher MSE value. In terms of file size, RSA tends to produce smaller files, while AES results in larger sizes. This research provides guidance for selecting encryption algorithms that meet the needs of specific applications, particularly in visual data security. These findings are expected to assist students and information security practitioners in determining the optimal algorithm to protect digital images from threats.

Keywords: Digital Image; RSA; AES; MSE; Data Security

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital ini telah mengubah banyak aspek kehidupan manusia, terutama dalam hal pengelolaan data digital yang semakin melimpah [1]. Data digital, seperti citra digital, kini dianggap sebagai aset berharga yang perlu dilindungi dari ancaman keamanan siber, seperti hacking dan pencurian identitas. Citra digital, yang banyak digunakan di bidang komunikasi, medis, dan keamanan, merupakan representasi

numerik dari gambar yang terdiri dari piksel-piksel dengan nilai warna tersendiri, memungkinkan gambar untuk diproses dan dimodifikasi secara digital [2]. Teknologi ini mempermudah pengeditan, distribusi, serta analisis data secara mendalam, sehingga menjadi elemen penting dalam kehidupan sehari-hari [3].

Citra digital dihasilkan melalui konversi sinyal analog menjadi sinyal digital melalui proses pengambilan sampel dan kuantisasi [4]. Proses ini menghasilkan matriks numerik yang merepresentasikan intensitas cahaya pada tiap titik gambar, memungkinkan manipulasi gambar secara efisien oleh komputer. Pengolahan citra digital telah membawa perubahan besar di berbagai bidang, mulai dari fotografi hingga dunia medis, serta membantu pemetaan wilayah melalui citra satelit dan drone [5]. Namun, pengolahan citra digital juga menghadapi tantangan, seperti gangguan noise dan kompresi berlebihan, yang mulai diatasi dengan kecerdasan buatan untuk analisis citra yang lebih presisi [6].

Untuk melindungi citra digital dari akses yang tidak sah, enkripsi menjadi solusi utama. Keamanan informasi melalui enkripsi sangat penting, terutama di dunia maya yang rentan terhadap serangan siber. Enkripsi dapat dilakukan dengan dua metode utama: enkripsi simetris yang menggunakan kunci rahasia, seperti *Advanced Encryption Standard* (AES), dan enkripsi asimetris yang menggunakan kunci publik dan privat, seperti RSA [7]. AES dikenal karena kecepatan dan efisiensinya dalam menangani data berukuran besar, sedangkan RSA, yang mengandalkan faktorisasi bilangan prima, terkenal karena tingkat keamanannya yang tinggi [8].

RSA, ditemukan pada tahun 1977, memanfaatkan prinsip faktorisasi bilangan prima untuk menghasilkan sepasang kunci publik dan privat yang digunakan dalam protokol keamanan seperti SSL dan TLS [9]. Di sisi lain, AES, yang diadopsi oleh NIST pada 2001, menggunakan kunci simetris dalam proses enkripsi dan dekripsi data. AES lebih efisien dalam menangani citra digital, sementara RSA sering menghadapi tantangan dalam mengenkripsi data berukuran besar, seperti citra digital. Meskipun kedua algoritma ini efektif, tantangan tetap ada, terutama dalam pengelolaan kunci enkripsi pada AES dan proses enkripsi data besar pada RSA [10].

Penelitian sebelumnya yang dilakukan oleh Alsaffar, dkk. (2020) menguji AES dan RSA dalam enkripsi citra digital dengan fokus pada kualitas enkripsi tanpa membahas kecepatan atau efisiensi sumber daya. Penggunaan MATLAB dalam eksperimen tersebut juga membatasi hasil yang diperoleh. Oleh karena itu, penelitian ini bertujuan untuk membandingkan kinerja algoritma RSA dan AES dalam enkripsi dan dekripsi citra digital menggunakan format PNG, dengan fokus pada kecepatan enkripsi, kualitas citra yang dihasilkan, serta ukuran file. Penelitian ini diharapkan dapat memberikan wawasan penting dalam memilih algoritma enkripsi yang optimal untuk perlindungan data visual.

Dengan semakin meningkatnya kebutuhan akan perlindungan citra digital, hasil penelitian ini diharapkan dapat membantu pengembang dan praktisi keamanan informasi dalam memilih algoritma enkripsi yang tepat. Selain itu, penelitian ini juga diharapkan dapat memberikan kontribusi bagi pengembangan teknologi enkripsi, khususnya dalam pengolahan citra digital, dan meningkatkan kesadaran akan pentingnya perlindungan data visual di era digital ini.

METODE

Jenis penelitian ini menggunakan pendekatan kuantitatif eksperimental [11] yang bertujuan untuk membandingkan kinerja dua algoritma kriptografi, yaitu RSA dan AES, dalam enkripsi citra digital. Penelitian ini akan mengevaluasi kedua algoritma berdasarkan beberapa parameter, antara lain kecepatan enkripsi dan dekripsi, kualitas citra setelah dekripsi yang diukur

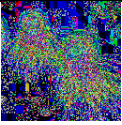



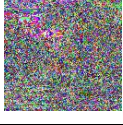

menggunakan *Mean Squared Error* (MSE), serta tingkat keamanan yang dihasilkan oleh masing-masing algoritma. Pendekatan kuantitatif dipilih untuk memberikan analisis yang objektif dan terukur terhadap data yang diperoleh [12]. Variabel bebas dalam penelitian ini adalah algoritma enkripsi yang digunakan, yaitu RSA dan AES, sementara variabel terikat mencakup kinerja algoritma yang diukur melalui waktu pemrosesan (kecepatan enkripsi dan dekripsi), kualitas citra yang dihasilkan setelah enkripsi (dengan MSE), dan ukuran file hasil enkripsi dan dekripsi. Pendekatan ini memungkinkan perbandingan yang sistematis antara kedua algoritma, sehingga menghasilkan temuan yang dapat dipertanggungjawabkan secara ilmiah.

HASIL DAN PEMBAHASAN





Hasil pengolahan data yang telah dilakukan setelah pengujian enkripsi dan dekripsi pada citra digital menggunakan algoritma RSA dan AES. Citra digital dibagi menjadi dua resolusi, yakni ukuran 128×128 piksel dan 256×256 piksel.

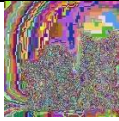

1. Hasil Pengujian Algoritma RSA

Tabel 1 Data Enkripsi dan Dekripsi Algoritma RSA
Citra Resolusi 128×128 piksel

No	Nama Citra Digital	Hasil enkripsi algoritma RSA	Waktu enkripsi (detik)	Ukuran file enkripsi (kb)	Hasil dekripsi algoritma RSA	Waktu dekripsi (detik)	Ukuran file dekripsi (kb)
1	Gambar_1		0,1443	35,23		0,1426	25,85
2	Gambar_2		0,1671	46,20		0,1822	37,59
3	Gambar_3		0,1557	46,14		0,1485	29,86

Tabel 2 Data Enkripsi dan Dekripsi Algoritma RSA
Citra Resolusi 256×256 piksel







No	Nama Citra Digital	Hasil enkripsi algoritma RSA	Waktu proses enkripsi (detik)	Ukuran file enkripsi (kb)	Hasil dekripsi algoritma RSA	Waktu proses dekripsi (detik)	Ukuran file dekripsi (kb)
1	Gambar_1		0,5107	100,39		0,6355	58,27
2	Gambar_2		0,5242	188,31		0,6114	134,63

3	Gambar_3		0,5625	100,26		0,6330	60,80
---	----------	---	--------	--------	--	--------	-------


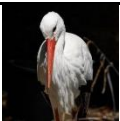
Hasil pengujian enkripsi dan dekripsi citra digital menggunakan algoritma RSA menunjukkan pengaruh resolusi citra terhadap waktu pemrosesan dan ukuran file yang dihasilkan. Pada citra 128×128 piksel (Tabel 1), waktu rata-rata enkripsi adalah 0,1448 detik dan dekripsi 0,1620 detik, dengan ukuran file enkripsi rata-rata 44,33 kb dan dekripsi 30,75 kb. Proses enkripsi lebih cepat daripada dekripsi, dan ukuran file dekripsi sedikit lebih kecil. Pada citra 256×256 piksel (Tabel 2), waktu enkripsi rata-rata meningkat menjadi 0,5691 detik, sementara dekripsi membutuhkan 0,6806 detik. Ukuran file enkripsi rata-rata adalah 147,30 kb, dan dekripsi 91,93 kb. Peningkatan resolusi citra menyebabkan waktu pemrosesan lebih lama dan ukuran file lebih besar. Secara keseluruhan, algoritma RSA menunjukkan kinerja yang baik, dengan waktu dekripsi sedikit lebih lama dan variasi ukuran file antara enkripsi dan dekripsi, seiring meningkatnya resolusi citra.





2. Hasil Pengujian Algoritma AES

Tabel 3 Data Enkripsi dan Dekripsi Algoritma AES
Citra Resolusi 128 × 128 piksel

No	Nama Citra Digital	Hasil enkripsi algoritma RSA	Waktu proses enkripsi (detik)	Ukuran file enkripsi (kb)	Hasil dekripsi algoritma RSA	Waktu proses dekripsi (detik)	Ukuran file dekripsi (kb)
1	Gambar_1		0,0040	48,20		0,0048	25,85
2	Gambar_2		0,0032	48,20		0,0032	37,59
3	Gambar_3		0,0037	48,20		0,0042	29,86

Tabel 4 Data Enkripsi dan Dekripsi Algoritma AES
Citra Resolusi 128 × 128 piksel

No	Nama Citra Digital	Hasil enkripsi algoritma RSA	Waktu proses enkripsi (detik)	Ukuran file enkripsi (kb)	Hasil dekripsi algoritma RSA	Waktu proses dekripsi (detik)	Ukuran file dekripsi (kb)
1	Gambar_1		0,0163	192,55		0,0120	58,27

2	Gambar_2		0,0148	192,55		0,0163	134,63
3	Gambar_3		0,0133	192,55		0,0122	60,80

Hasil pengujian enkripsi dan dekripsi citra digital menggunakan algoritma AES menunjukkan bahwa resolusi citra mempengaruhi waktu pemrosesan, ukuran file, dan kualitas citra. Pada citra 128×128 piksel (Tabel 3), waktu enkripsi rata-rata adalah 0,0053 detik dan dekripsi 0,0044 detik, dengan ukuran file enkripsi rata-rata 48,20 kb dan dekripsi 30,76 kb. Proses dekripsi sedikit lebih cepat daripada enkripsi, dan ukuran file dekripsi lebih kecil. Pada citra 256×256 piksel (Tabel 4), waktu enkripsi rata-rata adalah 0,0151 detik, sementara dekripsi membutuhkan 0,0160 detik. Ukuran file enkripsi rata-rata adalah 192,55 kb, dan file dekripsi rata-rata 91,93 kb. Secara keseluruhan, algoritma AES menunjukkan efisiensi tinggi dalam pemrosesan citra, dengan waktu pemrosesan yang sedikit lebih lama pada citra beresolusi lebih tinggi, namun tetap konsisten dalam ukuran file enkripsi. Ukuran file dekripsi cenderung lebih kecil dibandingkan dengan enkripsi.

3. Hasil Pengujian MSE untuk Citra Terenkripsi

Tabel 5 Hasil MSE Citra Terenkripsi

No	MSE citra enkripsi algoritma RSA		MSE citra enkripsi algoritma AES	
	128×128 Piksel	256×256 Piksel	128×128 Piksel	256×256 Piksel
1	10669,9	13832,4	17134,3	17065,1
2	8532,6	8813,9	8791,0	8919,0
3	7581,0	8393,8	8550,9	9833,3

Hasil pengujian MSE (*Mean Squared Error*) pada citra digital menggunakan algoritma RSA dan AES menunjukkan perbedaan nilai MSE berdasarkan resolusi citra. Pada RSA, citra dengan resolusi 128×128 piksel memiliki MSE rata-rata 9640,8, sementara pada resolusi 256×256 piksel, MSE meningkat menjadi 10826,9, menunjukkan perbedaan yang lebih besar antara citra asli dan hasil enkripsi pada resolusi lebih tinggi. Pada AES, MSE untuk citra 128×128 piksel memiliki rata-rata 10311,0, sedangkan pada resolusi 256×256 piksel, MSE sedikit lebih tinggi, yaitu 11180,3. Peningkatan MSE pada algoritma mengindikasikan bahwa semakin tinggi resolusi citra, semakin besar perbedaan antara citra asli dan hasil enkripsi akibat kompleksitas data yang lebih tinggi [14].

4. Hasil Keseluruhan Perbandingan Kinerja Algoritma

Tabel 6 Data Keseluruhan Hasil Kinerja Algoritma RSA dan AES

Resolusi	Algoritma	Kecepatan Enkripsi	Kecepatan Dekripsi	Ukuran Hasil Enkripsi	Ukuran Hasil Dekripsi	Nilai MSE
128	RSA	M: 0,1448	M: 0,1620	M: 44,33	M: 30,75	M: 9640,8
		Me: 0,1417	Me: 0,1634	Me: 46,12	Me: 31,02	Me: 9434,3
		R: 0,0480	R: 0,0396	R: 12,43	R: 15,47	R: 5238,0
	AES	M: 0,0053	M: 0,0044	M: 48,20	M: 30,76	M: 10311,0
		Me: 0,0052	Me: 0,0040	Me: 48,20	Me: 31,02	Me: 9781,8
		R: 0,0053	R: 0,0038	R: 0,00	R: 15,47	R: 9445,7
256	RSA	M: 0,5691	M: 0,6806	M: 147,30	M: 91,93	M: 10826,9
		Me: 0,5473	Me: 0,6709	Me: 152,53	Me: 89,19	Me: 9827,6
		R: 0,3086	R: 0,3265	R: 98,18	R: 100,83	R: 13581,0
	AES	M: 0,0151	M: 0,0160	M: 192,55	M: 91,93	M: 11180,3
		Me: 0,0148	Me: 0,0174	Me: 192,55	Me: 89,19	Me: 10222,5
		R: 0,0067	R: 0,0163	R: 0,00	R: 100,75	R: 12661,1

AES unggul dalam efisiensi waktu enkripsi dan dekripsi dibandingkan RSA. Pada resolusi 128×128, AES jauh lebih cepat dengan waktu enkripsi 0,0053 detik dan dekripsi 0,0044 detik, sementara RSA membutuhkan masing-masing 0,1448 detik dan 0,1620 detik. Pada resolusi 256×256, perbedaan waktu semakin mencolok, dengan AES memproses lebih cepat (0,0151 detik enkripsi, 0,0160 detik dekripsi) dibandingkan RSA (0,5691 detik enkripsi, 0,6806 detik dekripsi). Dalam hal ukuran file enkripsi, RSA menghasilkan ukuran lebih kecil, namun AES lebih konsisten dengan rentang ukuran yang lebih kecil. Menurut studi sebelumnya, AES dikenal memiliki kecepatan lebih tinggi karena sifat algoritmanya yang berbasis simetri, sehingga lebih efisien dalam proses komputasi untuk data yang lebih besar [13]. MSE untuk RSA sedikit lebih rendah dibandingkan AES pada kedua resolusi, namun AES menunjukkan variasi MSE yang lebih kecil, menandakan kestabilan kualitas enkripsi. Sebuah penelitian juga menyebutkan bahwa algoritma RSA cenderung menghasilkan data terenkripsi yang lebih kecil karena struktur matematisnya yang berbeda dibandingkan AES [14]. Selain itu, [15] menjelaskan bahwa desain AES yang berbasis pada substitusi dan permutasi blok data memberikan keunggulan signifikan dalam kecepatan enkripsi pada berbagai ukuran data. Secara keseluruhan, AES lebih cocok untuk aplikasi yang memprioritaskan kecepatan dan konsistensi, sementara RSA lebih efisien untuk aplikasi yang membutuhkan penghematan ruang penyimpanan dan kualitas enkripsi yang sedikit lebih baik. Pemilihan algoritma tergantung pada kebutuhan spesifik aplikasi.

KESIMPULAN

Berdasarkan hasil dan pembahasan diatas, AES terbukti lebih cepat dalam proses enkripsi dan dekripsi dibandingkan RSA. Pada citra 128×128 piksel, AES hanya membutuhkan 0,0053 detik untuk enkripsi dan 0,0044 detik untuk dekripsi, sedangkan RSA memerlukan 0,1448 detik dan 0,1620 detik. Perbedaan waktu pemrosesan semakin mencolok pada citra 256×256 piksel, di

mana AES memproses lebih cepat (0,0151 detik untuk enkripsi dan 0,0160 detik untuk dekripsi) dibandingkan RSA (0,5691 detik dan 0,6806 detik). Meskipun AES menghasilkan file terenkripsi yang lebih besar, sekitar 192,55 kb untuk citra 256×256 piksel dengan ukuran yang konsisten (rentang 0,00 kb), RSA menghasilkan file lebih kecil dengan rata-rata 147,30 kb, namun dengan variasi yang lebih besar. Ukuran file hasil dekripsi dari kedua algoritma lebih kecil dibandingkan file terenkripsi, dengan AES mempertahankan konsistensi ukuran, sementara RSA menunjukkan sedikit perubahan pada ukuran file dekripsi. Dari sisi kualitas enkripsi, AES memiliki nilai MSE yang lebih tinggi daripada RSA, yang menunjukkan perubahan struktur citra yang lebih signifikan. Pada citra 128×128 piksel, MSE enkripsi AES tercatat 10311,0, sedangkan RSA 9640,8, dan pada citra 256×256 piksel, MSE enkripsi AES mencapai 11180,3, sedikit lebih tinggi dibandingkan RSA yang memiliki nilai 10826,9.

DAFTAR PUSTAKA

- [1] Ginting, A., Isnanto, R. R., & Windasari, I. P. (2015). *Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email*. *Jurnal Teknologi Dan Sistem Komputer*, 3, 253–258.
- [2] Cahyanti, M., Salim, R. A., & Wisuda, M. (2016). *Implementasi Pengolahan Citra Untuk Pengenalan Citra Bendera Negara Berdasarkan Warna*. In *Seminar Riset Teknologi Informasi (SRITI)*.
- [3] Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, O. D., & Wijanarto. (2009). *Teori Pengolahan Citra Digital*. Andi Offset.
- [4] Purnama, A. (2015). *Aplikasi Matriks dan Pengolahan Gambar*. ResearchGate. Retrieved from https://www.researchgate.net/publication/302909688_Aplikasi_Matriks_dalam_Pengolahan_Gambar.
- [5] Kusumanto, R. D., & Tompunu, A. N. (2011). *Pengolahan Citra Digital Untuk Mendeteksi Objek Menggunakan Pengolahan Warna Model Normalisasi RGB*. In *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*.
- [6] Kuznetsov, Y. V. (2021). *Image Sampling, Quantization, and Encoding*. In *Springer eBooks* (pp. 127–149). https://doi.org/10.1007/978-3-030-60955-9_6.
- [7] Belkaid, B. M. (2015). *Encryption of Meteosat images using AES and RSA algorithms*. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 6(6).
- [8] Venkatesha, G., Dinesh, S., & Manjunath, M. (2019). *AES-based algorithm for image encryption and decryption*. *Perspectives in Communication, Embedded-Systems and Signal-Processing - PiCES*, 2(11), 342-345. Retrieved from <http://pices-journal.com/ojs/index.php/pices/article/view>.
- [9] Gollagi, S. G., Srividya, R., Kumar, G. S., & Pareek, P. K. (2021). *A novel method for secure image encryption using an enhanced RSA algorithm*. *Proceedings of the 2021 International Conference on Frontiers in Applied and Theoretical Sciences (FATS)*. <https://doi.org/10.1109/fabs52071.2021.9702550>.
- [10] Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Fahhad Alqahtani, H., Alqahtani, N. N., Mohammed Alshammari, G., & Ali, A. A. (2020). *Image encryption using AES and RSA algorithms*. *Proceedings of the 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. <https://doi.org/10.1109/iccais48893.2020.9096809>.
- [11] Anshori, M., & Iswati, S. (2019). *Metodologi Penelitian Kuantitatif: Edisi 1*. Airlangga University Press.

- [12] Hamid, A dan Prasetyowati, R. A. (2022). Metodologi Penelitian Kualitatif, Kuantitatif dan Eksperimen. Literasi Nusantara Abadi Malang.
- [13] Berent, Adam (2016). *Advanced Encryption Standard by Example*. ABI Software Development.
- [14] Sahoo, A., Mohanty, P., & Sethi, P. C. (2022). *Image encryption using the RSA algorithm*. In *Lecture Notes in Networks and Systems* (pp. 641–652). https://doi.org/10.1007/978-981-19-0901-6_56.
- [15] Arrañaga, J. D. R., Chavarin, J. A. S., Panduro, J. J. R., & Alvarez, E. C. B. (2017). *Calculation for Rijndael-AES based on artificial neural networks*. Redalyc. Retrieved from <https://www.redalyc.org/journal/5122/512253718012/html>.