ANALISIS KINERJA ALGORITMA RSA PADA ENKRIPSI CITRA DIGITAL BERDASARKAN PARAMETER PSNR DAN MSE

[1]Jamaluddin, [2]Darwis R. Manalu, [3]Paska Marto Hasugian, [4]Roni J. Simamora
[1,2,4]Universitas Methodist Indonesia, Medan, Indonesia
[3]Universitas Katolik Santo Thomas, Medan, Indonesia

jamaluddin@methodist.ac.id

ABSTRACT

Digital image security is an important issue in this era of increasingly massive multimedia-based data exchange, especially for sensitive information that requires a high level of protection. This study aims to analyze the performance of the Rivest Shamir Adleman (RSA) asymmetric cryptography algorithm in the digital image encryption process based on the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) parameters, as well as encryption and decryption times. The method used is a quantitative experiment on 30 digital images with varying resolutions (256×256, 512×512, and 1024×1024 pixels) and two RSA key lengths (1024-bit and 2048-bit). The test results show that the MSE value ranges from 0.001068 to 0.002620 and the PSNR value ranges from 75.08 to 78.34 dB, indicating that the decrypted images are of very high quality and close to the original images. However, the computation time increased significantly with increasing resolution and key length, with RSA 2048-bit taking almost twice as long as RSA 1024-bit. These findings show that the RSA algorithm is very effective in maintaining the integrity of digital images, but has limitations in terms of computational time efficiency, especially for high-resolution images. Therefore, a balance between security and performance is needed in practical implementation

***Kata kunci—RSA*, Digital Image Encryption, PSNR, MSE, Data Security, Asymmetric Cryptography.**

I. PENDAHULUAN

Perkembangan teknologi digital telah mendorong peningkatan signifikan dalam pertukaran data berbasis citra di berbagai sektor, seperti administrasi publik, pendidikan, keamanan, industri kreatif, dan layanan kesehatan. Citra digital kini tidak hanya berfungsi sebagai media visualisasi, tetapi juga sebagai representasi data yang mengandung informasi sensitif dan bernilai tinggi. Menurut [1], transformasi data ke dalam format digital memberikan kemudahan distribusi dan penyimpanan, namun sekaligus meningkatkan risiko manipulasi serta akses tidak sah. Dalam konteks administrasi publik, penggunaan citra digital seperti pindaian KTP atau dokumen identitas lainnya memerlukan perlindungan tingkat tinggi karena berpotensi disalahgunakan apabila tidak diamankan dengan mekanisme kriptografi yang memadai [2].

Di sektor kesehatan, keamanan citra rekam medis digital juga menjadi perhatian utama. [3] dan [4] menegaskan bahwa kebocoran data medis dapat menimbulkan konsekuensi hukum dan etis yang serius. Oleh karena itu, perlindungan terhadap citra digital tidak hanya menyangkut aspek kerahasiaan (confidentiality), tetapi juga integritas (integrity) dan autentikasi (authentication).

Kriptografi merupakan pendekatan utama dalam menjaga keamanan informasi digital. Salah satu algoritma kriptografi asimetris yang paling banyak digunakan adalah Rivest Shamir Adleman (RSA). RSA bekerja berdasarkan prinsip kesulitan faktorisasi bilangan prima besar dan menggunakan pasangan kunci publik serta privat untuk proses enkripsi dan dekripsi. [5] menjelaskan bahwa RSA memiliki keunggulan dalam manajemen kunci serta fleksibilitas implementasi pada berbagai jenis data, termasuk teks, citra, dan multimedia.

Dalam implementasinya pada citra digital, algoritma RSA bekerja dengan mengenkripsi nilai piksel berdasarkan operasi modular eksponensial. Proses ini menghasilkan citra terenkripsi yang secara visual tidak dapat dikenali, dan pada proses dekripsi diharapkan mampu mengembalikan citra asli secara utuh (lossless). Keberhasilan tersebut umumnya diukur menggunakan parameter kuantitatif seperti Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE). PSNR digunakan untuk mengukur tingkat kemiripan antara citra asli dan citra hasil dekripsi, sedangkan MSE mengukur tingkat kesalahan rata-rata antar piksel. Nilai PSNR yang tinggi dan MSE yang rendah menunjukkan tingkat integritas data yang baik [6].

Sejumlah penelitian menunjukkan bahwa RSA mampu menjaga integritas citra dengan sangat baik. [7] melaporkan nilai PSNR mencapai 100 dB pada hasil dekripsi citra KTP digital, yang mengindikasikan bahwa citra dapat dipulihkan secara sempurna. Namun demikian, studi komparatif oleh [6] menunjukkan bahwa meskipun RSA unggul dalam aspek keamanan asimetris dan ukuran file tertentu, algoritma ini memiliki kelemahan dalam efisiensi waktu komputasi dibandingkan algoritma simetris seperti AES. Hal ini menjadi tantangan terutama pada citra beresolusi tinggi yang memiliki jumlah piksel besar.

Selain itu, pengembangan metode hybrid seperti kombinasi RSA dengan XOR Cipher [7] maupun steganografi LSB dan EOF [8], [9] menunjukkan adanya upaya peningkatan performa dan efisiensi tanpa mengorbankan kualitas visual hasil dekripsi. Meskipun demikian, sebagian besar penelitian terdahulu lebih berfokus pada implementasi teknis atau pengembangan sistem tertentu, dan belum banyak yang melakukan analisis kinerja RSA secara spesifik berdasarkan

parameter objektif PSNR dan MSE sebagai indikator utama integritas citra.

Berdasarkan latar belakang tersebut, terdapat kebutuhan untuk melakukan analisis yang lebih sistematis terhadap kinerja algoritma RSA pada enkripsi citra digital dengan menitikberatkan pada parameter PSNR dan MSE. Analisis ini penting untuk memberikan gambaran empiris mengenai sejauh mana RSA mampu mempertahankan kualitas citra pasca-dekripsi serta mengidentifikasi implikasi performa komputasi dalam implementasi praktis.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis kinerja algoritma RSA dalam enkripsi citra digital berdasarkan parameter PSNR dan MSE guna memberikan kontribusi ilmiah terhadap pengembangan sistem keamanan citra digital yang efektif, terukur, dan relevan dengan kebutuhan keamanan informasi modern.

II. METODOLOGI PENELITIAN

A. Jenis dan Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental kuantitatif untuk menganalisis kinerja algoritma RSA pada proses enkripsi dan dekripsi citra digital. Desain eksperimen dilakukan dengan menerapkan algoritma RSA secara langsung pada sejumlah citra uji, kemudian mengevaluasi kualitas hasil dekripsi menggunakan parameter Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE).

Eksperimen dilakukan dalam lingkungan terkontrol untuk memastikan bahwa setiap citra diuji menggunakan parameter kunci RSA yang konsisten sehingga hasil dapat dibandingkan secara objektif.

B. Dataset dan Spesifikasi Citra Uji

Dataset yang digunakan dalam penelitian ini terdiri dari citra digital berformat JPEG dan PNG dengan variasi karakteristik sebagai berikut:

1. Citra grayscale
2. Citra RGB (24-bit color depth)
3. Resolusi rendah (256×256 piksel)
4. Resolusi menengah (512×512 piksel)
5. Resolusi tinggi (1024×1024 piksel)

Pemilihan variasi resolusi bertujuan untuk menguji pengaruh jumlah piksel terhadap waktu komputasi dan kualitas hasil dekripsi. Total citra uji yang digunakan sebanyak 30 citra, yang dibagi secara proporsional berdasarkan kategori resolusi dan tipe warna.

C. Teknik Analisis Data

Data hasil eksperimen dianalisis secara deskriptif kuantitatif dengan:

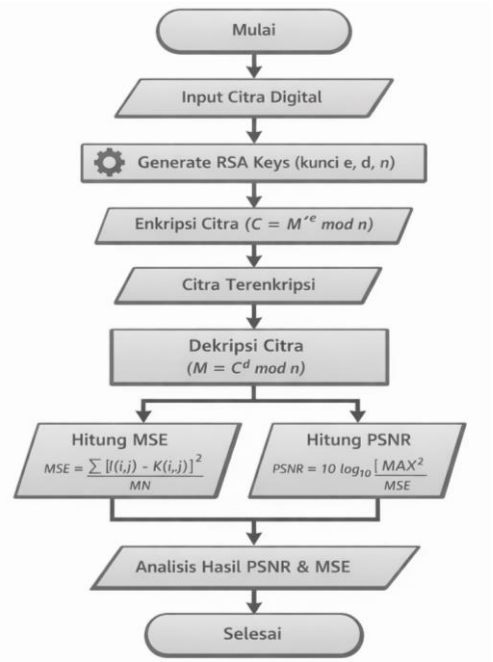
1. Menghitung rata-rata PSNR dan MSE untuk setiap kategori resolusi
2. Membandingkan performa kunci 1024-bit dan 2048-bit
3. Menganalisis hubungan antara resolusi citra dan waktu komputasi
4. Menentukan tingkat efektivitas RSA berdasarkan standar kualitas citra:
   - PSNR > 40 dB → kualitas sangat baik
   - MSE mendekati 0 → integritas tinggi

Hasil analisis kemudian disajikan dalam bentuk tabel dan grafik untuk memperjelas perbandingan performa algoritma.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis kinerja algoritma RSA dalam enkripsi citra digital berdasarkan parameter PSNR dan MSE guna memberikan kontribusi ilmiah terhadap pengembangan sistem keamanan citra digital yang efektif, terukur, dan relevan dengan kebutuhan keamanan informasi modern.

III. PERANCANGAN SISTEM

Perancangan diagram alir penelitian menggambarkan alur sistem mulai dari proses input citra hingga analisis hasil evaluasi menggunakan parameter PSNR dan MSE. Setiap tahapan dirancang untuk memastikan proses eksperimen berjalan sistematis, terukur, dan dapat direplikasi.



Gambar 1. Diagram Alir (*Flowchart*) Penelitian

Flowchart di atas menggambarkan alur penelitian dalam menguji kinerja algoritma RSA pada enkripsi citra digital. Proses dimulai dari tahap mulai, kemudian sistem menerima input berupa citra digital yang akan diuji. Citra tersebut dibaca dan diubah menjadi bentuk matriks piksel agar dapat diproses secara matematis.

Setelah citra dimasukkan, sistem melakukan pembuatan kunci RSA, yaitu menghasilkan pasangan kunci publik dan kunci privat. Kunci publik digunakan untuk melakukan proses enkripsi, sedangkan kunci privat digunakan untuk proses dekripsi.

Tahap berikutnya adalah enkripsi citra, di mana setiap nilai piksel pada citra diubah menggunakan rumus matematika RSA. Hasil dari proses ini adalah citra terenkripsi yang tampilannya sudah tidak dapat dikenali secara visual karena nilai pikselnya telah diacak.

Selanjutnya dilakukan proses dekripsi, yaitu mengembalikan citra terenkripsi ke bentuk aslinya menggunakan kunci privat. Jika algoritma bekerja dengan baik, citra hasil dekripsi akan sangat mirip dengan citra asli.

Untuk mengetahui tingkat keberhasilan proses tersebut, sistem menghitung dua parameter evaluasi, yaitu MSE (Mean Squared Error) dan PSNR (Peak Signal-to-Noise Ratio). MSE digunakan untuk mengukur seberapa besar perbedaan antara citra asli dan citra hasil

dekripsi. Semakin kecil nilai MSE, semakin kecil kesalahan yang terjadi. PSNR digunakan untuk mengukur kualitas citra hasil dekripsi dibandingkan citra asli. Semakin tinggi nilai PSNR, semakin baik kualitas citra tersebut.

Tahap terakhir adalah analisis hasil PSNR dan MSE untuk menentukan seberapa efektif algoritma RSA dalam menjaga integritas citra digital. Setelah seluruh proses selesai, penelitian dinyatakan berakhir.

IV. HASIL DAN PEMBAHASAN

A. Hasil Pengujian

Pengujian dilakukan terhadap 30 citra digital dengan variasi resolusi (256×256, 512×512, 1024×1024) dan dua panjang kunci RSA (1024-bit dan 2048-bit). Parameter yang dianalisis meliputi:

1. Mean Squared Error (MSE)
2. Peak Signal-to-Noise Ratio (PSNR)
3. Waktu Enkripsi
4. Waktu Dekripsi

Tabel 1. Hasil Pengujian Kinerja RSA pada Enkripsi Citra Digital

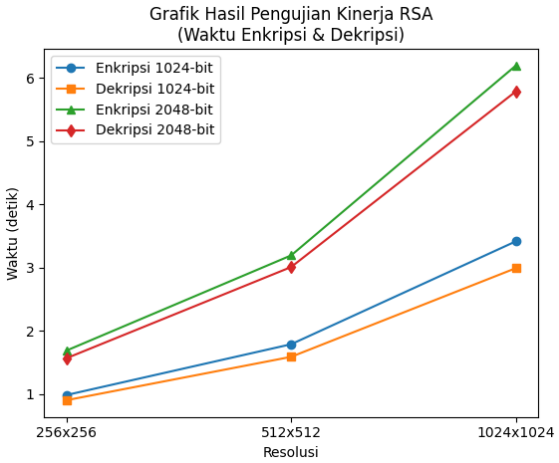
Resolusi	Panjang Kunci RSA	MSE	PSNR	Waktu Enkripsi (detik)	Waktu Dekripsi (detik)
256x256	1024	0.002620	75.08	988	906
256x256	2048	0.001068	78.34	1.691	1.570
512x512	1024	0.002389	75.83	1.791	1.592
512x512	2048	0.001689	76.23	3.196	3.012
1024x1024	1024	0.001941	77.60	3.418	2.994
1024x1024	2048	0.001619	76.26	6.197	5.788

Tabel diatas menyajikan hasil rata-rata pengujian kinerja algoritma RSA pada tiga variasi resolusi citra (256×256, 512×512, dan 1024×1024 piksel) dengan dua panjang kunci, yaitu 1024-bit dan 2048-bit. Berdasarkan hasil tersebut, nilai Mean Squared Error (MSE) berada pada rentang yang sangat kecil, yaitu antara 0,001068 hingga 0,002620. Nilai ini menunjukkan bahwa perbedaan antara citra asli dan citra hasil dekripsi sangat minimal. Sejalan dengan itu, nilai Peak Signal-to-Noise Ratio (PSNR) berada pada rentang 75,08 dB hingga 78,34 dB, yang secara umum dapat dikategorikan sebagai kualitas citra sangat baik. Tingginya nilai PSNR pada seluruh kombinasi resolusi dan panjang kunci mengindikasikan bahwa algoritma RSA mampu mengembalikan citra ke bentuk aslinya secara hampir sempurna tanpa distorsi visual yang berarti.

Dari sisi perbandingan panjang kunci, RSA 2048-bit cenderung menghasilkan nilai MSE yang sedikit lebih rendah dibandingkan 1024-bit, meskipun perbedaan nilai PSNR yang dihasilkan tidak terlalu signifikan. Hal ini menunjukkan bahwa peningkatan panjang kunci memberikan sedikit peningkatan presisi pada proses dekripsi, namun tidak berdampak besar terhadap kualitas visual citra hasil akhir. Dengan demikian, baik kunci 1024-bit maupun 2048-bit sama-sama mampu menjaga integritas citra secara optimal.

Sebaliknya, perbedaan yang cukup signifikan terlihat pada parameter waktu komputasi. Waktu enkripsi dan dekripsi meningkat seiring dengan bertambahnya resolusi citra. Pada resolusi 256×256, waktu enkripsi RSA 1024-bit tercatat sekitar 0,99 detik dan meningkat menjadi sekitar 3,42 detik pada resolusi 1024×1024. Pola serupa juga terjadi pada RSA 2048-bit, di mana waktu enkripsi meningkat dari sekitar 1,69 detik menjadi lebih dari 6 detik. Selain itu, penggunaan kunci 2048-bit secara konsisten menghasilkan waktu proses hampir dua kali lebih lama dibandingkan kunci 1024-bit. Hal ini menunjukkan bahwa kompleksitas komputasi RSA sangat dipengaruhi oleh panjang kunci dan jumlah piksel citra yang diproses.

Secara keseluruhan, hasil pada Tabel 2 menegaskan bahwa algoritma RSA sangat efektif dalam menjaga kualitas dan integritas citra digital berdasarkan parameter PSNR dan MSE, namun memiliki konsekuensi peningkatan waktu komputasi yang signifikan pada resolusi tinggi dan panjang kunci yang lebih besar. Temuan ini menunjukkan adanya trade-off antara tingkat keamanan dan efisiensi waktu, sehingga pemilihan panjang kunci perlu disesuaikan dengan kebutuhan sistem yang akan diimplementasikan.



Gambar 2. Grafik Hasil Pengujian Kinerja RSA Terhadap Tiga Variasi Resolusi Citra

B. Pembahasan

Berdasarkan hasil pengujian, kualitas citra hasil dekripsi pada semua variasi resolusi dan panjang kunci menunjukkan PSNR sangat tinggi (±75–78 dB) serta MSE sangat kecil (≈10^{-3}). Pola ini mengindikasikan bahwa proses dekripsi mampu mengembalikan citra mendekati kondisi asli (lossless secara praktis). Temuan ini sejalan dengan penelitian [6] dan [2] yang menunjukan PSNR sangat tinggi (hingga 100 dB) pada pengamanan citra menggunakan RSA, menegaskan bahwa pendekatan RSA (terutama bila dipadukan) sangat kuat dalam menjaga integritas visual data sensitif.

Jika dibandingkan dari sisi akurasi (PSNR/MSE), hasil pengujian juga konsisten dengan berbagai studi implementasi RSA pada objek citra yang menekankan pemulihan data yang baik setelah dekripsi. [5] menunjukkan penerapan RSA pada aplikasi enkripsi gambar dengan pemisahan kunci publik–privat, yang secara konseptual mendukung tujuan menjaga kerahasiaan sekaligus memungkinkan pemulihan data oleh pihak berwenang.

Namun, berbeda dengan kualitas citra yang stabil, waktu komputasi pada pengujian meningkat tajam saat resolusi bertambah, dan RSA 2048-bit secara konsisten lebih lambat daripada RSA 1024-bit. Tren ini sangat

sesuai dengan studi komparatif [6] yang menunjukkan bahwa RSA cenderung membutuhkan waktu pemrosesan lebih lama daripada algoritma simetris (misalnya AES), terutama karena operasi eksponensial modular dan overhead manajemen kunci asimetris. Dengan demikian, hasil pengujian memperkuat argumen bahwa RSA unggul pada integritas/keamanan, tetapi memiliki konsekuensi pada efisiensi waktu—yang makin terasa pada citra beresolusi tinggi.

Kecenderungan penurunan efisiensi pada file visual besar juga sejalan dengan penelitian [10] pada pengamanan lukisan digital, yang menyoroti bahwa pendekatan RSA dapat menjadi kurang efisien ketika ukuran/kompleksitas data meningkat. Ini menguatkan interpretasi bahwa kenaikan waktu enkripsi–dekripsi pada pengujian yang dilakukan bukan anomali, melainkan karakteristik umum RSA ketika diterapkan pada data citra dengan jumlah piksel besar.

Penggunaan PSNR dan MSE sebagai indikator utama evaluasi kualitas hasil dekripsi juga sesuai dengan literatur evaluasi enkripsi citra. [11] menegaskan PSNR (yang bergantung pada MSE) sebagai salah satu metrik yang umum dipakai untuk menilai perbedaan kualitas citra hasil pemrosesan/enkripsi terhadap citra asli. Hal ini memperkuat validitas metodologi evaluasi berbasis PSNR–MSE yang digunakan pada pengujian penelitian ini.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil pengujian terhadap 30 citra digital dengan variasi resolusi dan panjang kunci, dapat disimpulkan bahwa algoritma RSA menunjukkan kinerja yang sangat baik dalam menjaga integritas citra digital. Hal ini dibuktikan dengan nilai Mean Squared Error (MSE) yang sangat kecil serta nilai Peak Signal-to-Noise Ratio (PSNR) yang berada pada kategori sangat tinggi (di atas 75 dB), yang mengindikasikan bahwa citra hasil dekripsi hampir identik dengan citra asli. Peningkatan resolusi citra tidak memberikan pengaruh signifikan terhadap kualitas hasil dekripsi, namun berpengaruh langsung terhadap waktu komputasi. Selain itu, penggunaan kunci 2048-bit memberikan tingkat keamanan yang lebih tinggi dibandingkan 1024-bit, tetapi dengan konsekuensi peningkatan waktu enkripsi dan dekripsi yang cukup signifikan. Dengan demikian, algoritma RSA terbukti efektif dalam menjaga kualitas dan keamanan citra digital, meskipun memiliki keterbatasan pada aspek efisiensi waktu komputasi, terutama pada citra beresolusi tinggi.

B. Saran

Berdasarkan temuan penelitian ini, disarankan agar implementasi algoritma RSA pada sistem pengamanan citra digital mempertimbangkan keseimbangan antara tingkat keamanan dan efisiensi komputasi, khususnya dalam pemilihan panjang kunci sesuai kebutuhan aplikasi. Untuk citra beresolusi tinggi atau sistem yang memerlukan pemrosesan real-time, pendekatan hybrid seperti kombinasi RSA dengan algoritma simetris (misalnya AES) atau teknik optimasi paralel dapat dipertimbangkan untuk meningkatkan efisiensi waktu tanpa mengurangi tingkat keamanan. Selain itu, penelitian selanjutnya disarankan untuk menguji performa RSA pada lingkungan perangkat dengan sumber daya terbatas, serta mengevaluasi parameter tambahan seperti penggunaan memori dan ketahanan terhadap skenario serangan kriptanalisis yang lebih kompleks, guna memperoleh gambaran yang lebih komprehensif mengenai efektivitas algoritma RSA dalam pengamanan multimedia modern.

VI. REFERENSI

[1] Z. Deskiva, "Implementasi Kriptografi Modern Dengan Metode Rsa Pada Data Citra Digital," *Publikasi Ilmiah Teknologi Informasi Neumann*, vol. 3, no. 1, pp. 44–49, 2018.

[2] C. Repi, J. Titaley, and E. Ketaren, "Implementasi Kriptografi dalam Pengamanan Data Gambar Menggunakan Algoritma RSA," *Jurnal TIMES*, vol. 13, no. 1, pp. 93–99, Jul. 2024, doi: 10.51351/jtm.13.1.2024750.

[3] D. T. Tobing, "Implementasi Algoritma Rivest Shamir Adleman (RSA) untuk Keamanan Data Rekam Medik Penyakit Pasien Rumah Sakit," *Jurnal Kajian Ilmiah Teknologi Informasi dan Komputer*, vol. 2, no. 2, pp. 65–73, May 2024, doi: 10.62866/jutik.v2i2.131.

[4] S. Sutejo, "Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien," *INTECOMS: Journal of Information Technology and Computer Science*, vol. 4, no. 1, pp. 104–114, Jun. 2021, doi: 10.31539/intecoms.v4i1.2437.

[5] A. Khamsyar and Muh. Basri, "Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) Rsa," *Jurnal Sintaks Logika*, vol. 2, no. 3, pp. 39–45, Oct. 2022, doi: 10.31850/jsilog.v2i3.1850.

[6] M. S. R. Karim, M. Khudzaifah, and F. Rozi, "Studi Komparatif Algoritma RSA dan AES pada Enkripsi dan Dekripsi Citra Digital," *Jurnal Riset Mahasiswa Matematika*, vol. 4, no. 2, pp. 74–81, Feb. 2025, doi: 10.18860/jrmm.v4i2.31191.

[7] G. K. S. Artajaya and A. Muliantara, "Implementasi Kriptografi RSA dan XOR Cipher untuk Enkripsi Citra Digital KTP," *Jurnal Nasional Teknologi Informasi dan Aplikasinya*, vol. 2, no. 4, pp. 665–672, 2024.

[8] D. S. Milania, "Implementasi kriptografi RSA dan steganografi LSB dalam penyisipan pesan pada citra digital," Skripsi, Universitas Islam Negeri Maulana Malik Ibrahim, 2024.

[9] A. Malvi and P. Painem, "Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF)," *Informatik: Jurnal Ilmu Komputer*, vol. 16, no. 2, p. 67, Aug. 2020, doi: 10.52958/iftk.v16i2.1860.

[10] I. D. G. P. A. Biara and I. P. G. H. Suputra, "Sistem Pengamanan Lukisan Digital Menggunakan Metode Rivest Shamir Adleman (RSA)," *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, vol. 11, no. 4, p. 681, Apr. 2023, doi: 10.24843/JLK.2023.v11.i04.p05.

[11] M. K. Hussein, K. R. Hassan, and H. M. Al-Mashhadi, "The quality of image encryption techniques by reasoned logic," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 6, p. 2992, Dec. 2020, doi: 10.12928/telkomnika.v18i6.14340.