SINTA Jurnal Sistem Informasi dan Teknologi Komputasi
Volume 2 Nomor 2 April 2025 [page: 51-56]
DOI: https://doi.org/10.61124/sinta.v2i2.45

PERANCANGAN GUI MATLAB UNTUK KEAMANAN CITRA RGB MENGGUNAKAN ALGORITMA ACM DAN METODE LSB DALAM BERBAGAI UKURAN

Andre Dugarai Sam De Yosep*[1], Samy Y. Doo[1], Molina Olivia Odja[1]
[1]Program Studi Teknik Elektro, Universitas Nusa Cendana, Indonesia
[2]Program Studi Kedua dan Ketiga misalnya sama, Universitas Dua, Negara
*e-mail: andredugarai1661@gmail.com

Abstrak
Keamanan citra digital merupakan aspek penting dalam pertukaran informasi, terutama dengan meningkatnya ancaman siber. Penelitian ini bertujuan untuk mengembangkan sistem keamanan citra RGB berbasis GUI MATLAB dengan menggabungkan kriptografi *Arnold Cat Map* (ACM) dan steganografi *Least Significant Bit* (LSB) untuk keamanan berlapis. Kedua teknik ini mengatasi keterbatasan penggunaan satu teknik keamanan, dimana ACM menjamin citra terenkripsi sedangkan LSB membuat citra tidak dicurigai mengandung pesan rahasia. Metode penelitian meliputi studi literatur, implementasi algoritma, dan pengujian pada 25 citra dengan berbagai ukuran (100x100 hingga 500x500). Prosesnya adalah citra asli dienkripsi menggunakan algoritma ACM, citra terenkripsi disisipkan ke dalam citra wadah menggunakan metode LSB, dilanjutkan dengan proses dekripsi, dan pengujian MSE dan PSNR untuk mengukur kualitas dan integritas data. Hasil penelitian menunjukkan bahwa citra hasil dekripsi identik dengan citra asli (MSE=0, PSNR=inf), membuktikan keefektifan algoritma dalam memulihkan data. Nilai MSE yang rendah (0,002–0,049) dan PSNR yang tinggi (140–173 dB) pada citra wadah menunjukkan distorsi yang minimal. Waktu pemrosesan meningkat seiring dengan ukuran citra (22,6 detik untuk 100×100 menjadi 474,2 detik untuk 500×500), konsisten dengan kompleksitas komputasi yang diharapkan. Penelitian ini memberikan kontribusi berupa solusi keamanan hybrid yang menggabungkan keunggulan kriptografi dan steganografi, serta GUI yang *user-friendly* untuk kemudahan implementasi. Hasil penelitian ini dapat memberikan kontribusi terhadap informasi yang memerlukan tingkat keamanan ekstra dan penelitian lebih lanjut terkait waktu pemrosesan dengan penggunaan perangkat yang mumpuni.

Kata kunci: arnold cat map; least significant beat; kriptografi; steganografi; GUI MATLAB.

Abstract
Digital image security is important in information exchange, especially with the increasing cyber threats. This study aims to develop a GUI MATLAB-based RGB image security system by combining Arnold Cat Map (ACM) cryptography and Least Significant Bit (LSB) steganography for layered protection. These two techniques overcome the limitations of using one security technique, where ACM guarantees encrypted images while LSB makes the image not suspect of containing secret messages. The research method includes literature studies, algorithm implementation, and testing on 25 images of various sizes (100 × 100 to 500 × 500). The stages are the original image being encrypted using the ACM algorithm, the encrypted image being inserted into the container image using the LSB method, followed by the decryption process, and MSE and PSNR testing to measure data quality and integrity. The results show that the decrypted image is identical to the original (MSE = 0, PSNR = inf), proving the algorithm's effectiveness in recovering data. Low MSE values (0.002–0.049) and high PSNR (140–173 dB) in the container image indicate minimal distortion. The processing time increases with image size (22.6 s for 100×100 to 474.2 s for 500×500), consistent with the expected computational complexity. This study contributes a hybrid security solution that combines the advantages of cryptography and steganography, as well as a user-friendly GUI for easy implementation. The results of this study can contribute to information that needs an extra level of security and further research related to processing time with the use of qualified devices.

Keywords: arnold cat map; least significant beat; cryptography; steganography; GUI MATLAB.

1. PENDAHULUAN

Di era modern ini, citra merupakan media yang lebih akurat untuk bertukar informasi dibandingkan pesan teks. Banyak orang berpendapat bahwa citra dapat menjadi acuan untuk menentukan kebenaran suatu informasi. Oleh karena itu, informasi yang tidak disertai dengan bukti berupa citra dianggap tidak sah. Mengingat hal tersebut, beberapa citra harus dilindungi agar pihak yang tidak berwenang tidak menyalahgunakan informasi tersebut. Dengan demikian, keamanan citra menjadi hal yang krusial, terutama jika citra tersebut dikirim melalui internet yang dianggap lebih efisien, cepat, dan ekonomis [1]. Namun, tanpa disadari, kondisi ini membuat citra menjadi lebih rentan terhadap pencurian, sehingga informasinya dapat disalahgunakan. Tindakan pencurian dan penyalahgunaan data melalui internet dikenal sebagai kejahatan dunia maya, di mana citra menjadi salah satu sasaran utamanya. Sehingga dengan mengintegrasikan kriptografi dan steganografi (LSB) dapat meningkatkan keamanan data citra [2].

DOI: https://doi.org/10.61124/sinta.v2i2.45

Kriptografi mengenkripsi informasi visual untuk mengamankan data, sementara steganografi menyembunyikan pesan rahasia dalam data sampul yang tidak berbahaya, seperti file video. Metode LSB (*Least Significant Bit*) secara khusus digunakan untuk menyematkan pesan terenkripsi ke dalam video, citra untuk meningkatkan keamanan [2][3]. Pendekatan gabungan ini meningkatkan keamanan data, kapasitas, dan ketahanan terhadap akses yang tidak sah[4].

Penelitian mengenai kombinasi kriptografi dan steganografi telah dilakukan sebelumnya, seperti penelitian oleh Varly M. Ndolu yang mengombinasikan metode pengamanan data menggunakan kriptografi hill cipher dan steganografi least significant bit (LSB) pada citra digital. Hasil dari kombinasi metode tersebut menunjukkan kinerja yang baik, di mana citra stego tampak seperti citra asli, sehingga sangat sulit untuk dibedakan [5]. Penelitian lain dilakukan oleh Noor Ageng Setiyanto dkk, yang melakukan pengacakan citra digital berwarna dengan kriptografi arnold cat map (ACM). Hasil enkripsi pada sejumlah iterasi yang berbeda menghasilkan visualisasi citra yang bervariasi, penelitian ini bertujuan untuk mengkaji model dan pola pengacakan piksel pada hasil visualisasi citra hasil enkripsi [6]. Penelitian lainnya dilakukan oleh Ronsen Purba dkk, yang menggunakan dua algoritma enkripsi, yaitu algoritma arnold cat map (ACM) dan nonlinear chaotic algorithm (NCA). Proses enkripsi mencakup pengacakan susunan piksel menggunakan ACM, pengacakan nilai RGB, dan perubahan nilai dalam citra dengan memanfaatkan bilangan acak yang telah dihasilkan menggunakan NCA. Hasil pengujian menunjukkan bahwa citra yang terenkripsi memiliki distribusi intensitas piksel yang seragam dengan nilai koefisien korelasi yang rendah antara piksel-piksel yang berdekatan [7]. Penelitian ini bertujuan untuk merancang dan mengimplementasikan algoritma ACM dan metode LSB untuk keamanan data citra RGB dalam berbagai ukuran menggunakan GUI MATLAB.

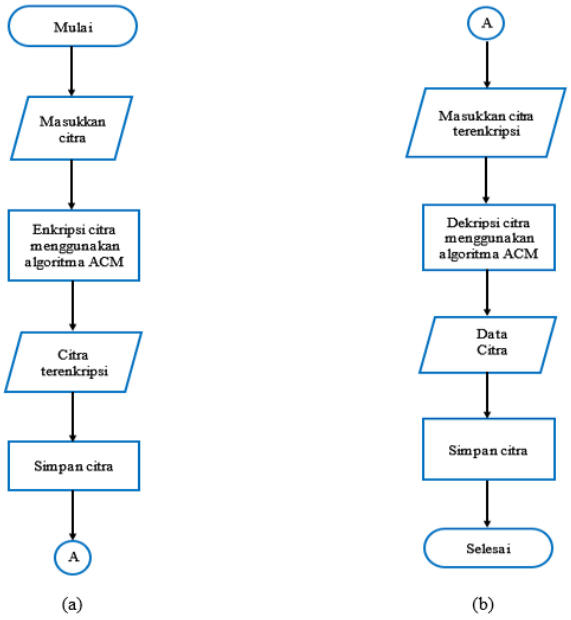
2. METODE

Metode yang digunakan dalam penelitian ini adalah kuantitatif sedangkan analisis data yang digunakan adalah deskriptif. Adapun pengumpulan data dimulai dengan melakukan studi literatur, perancangan dan implementasi serta pengujian sistem berbasis GUI Matlab.

A. Studi Literatur

Pada tahap ini dilakukan pencarian dan mempelajari literatur yang berhubungan dengan kriptografi dan steganografi pada citra, algoritma ACM dan metode LSB yang dapat diperoleh melalui buku, artikel ilmiah, penelitian terdahulu serta internet.

B. Perancangan Sistem GUI Matlab



Gambar 1. Diagram Alir (a) Proses Enkripsi Citra, (b) Proses Dekripsi Citra

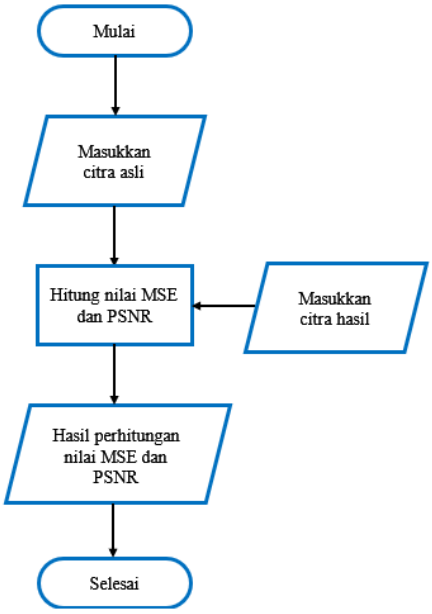
Perancangan sistem dilakukan dalam beberapa tahap yang disajikan dalam bentuk diagram alir sistem. Diagram alir sistem terdiri dari proses enkripsi menggunakan algoritma ACM (Gambar 1(a)), setelah citra

SINTA Jurnal Sistem Informasi dan Teknologi Komputasi
Volume 2 Nomor 2 April 2025 [page: 51-56]
DOI: https://doi.org/10.61124/sinta.v2i2.45

asli terenkripsi dilanjutkan dengan proses penyisipan citra terenkripsi kedalam citra wadah menggunakan metode LSB, selanjutnya adalah proses ekstraksi (mengambil kembali citra terenkripsi dari citra wadah) dan terakhir melakukan dekripsi terhadap citra tersebut (Gambar (b)).

C. Pengujian Sistem GUI Matlab

Pengujian dilakukan dengan menghitung nilai MSE dan PSNR dari citra. Proses perhitungan dilakukan dengan membandingkan citra asli (sebelum enkripsi) dan citra dekripsi untuk mengetahui kualitas dari citra. Diagram alir pengujian dapat dilihat pada Gambar 3.

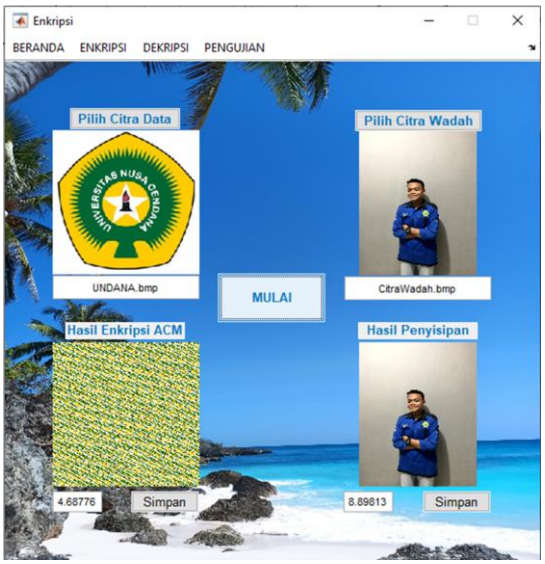


Gambar 2. Diagram Alir Pengujian Sistem

3. HASIL PENELITIAN

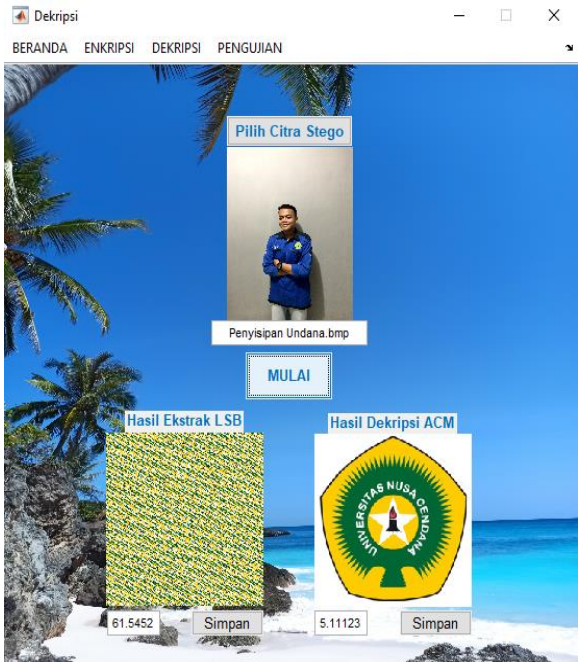
A. Hasil Perancangan Sistem Berbasis GUI Matlab

Perancangan sistem berbasis GUI Matlab dilakukan dalam beberapa tahapan, dimana yang pertama adalah proses enkripsi citra masukan atau citra asli (Gambar 1) kemudian dilanjutkan dengan proses menyisipkan citra hasil enkripsi pada citra wadah, selanjutnya dilakukan ekstraksi kemudian dekripsi (Gambar 2).



Gambar 1. Tampilan GUI Proses Enkripsi

SINTA Jurnal Sistem Informasi dan Teknologi Komputasi
Volume 2 Nomor 2 April 2025 [page: 51-56]
DOI: https://doi.org/10.61124/sinta.v2i2.45

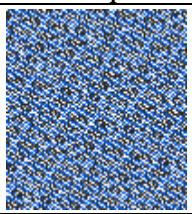
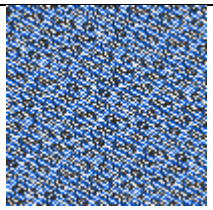
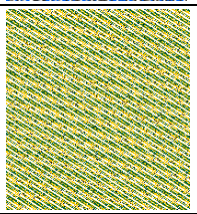
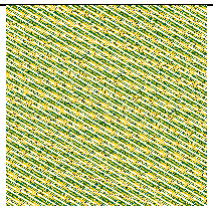
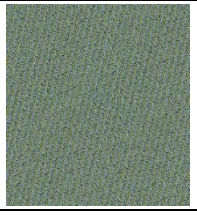
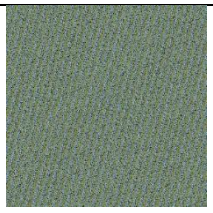


Gambar 2. Tampilan GUI Proses Dekripsi

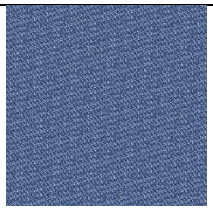
B. Hasil Implementasi Kombinasi Algoritma ACM dan Metode LSB

Implementasi kombinasi algoritma ACM dan metode LSB dilakukan pada 25 sampel citra RGB dengan ukuran yang berbeda-beda yaitu 100x100, 200x200, 300x300, 400x400 dan 500x500 dengan masing-masing ukuran sebanyak 5 citra. Tetapi pada artikel ini hanya disajikan masing-masing satu citra untuk setiap ukuran. Hasil dari implementasi algoritma ACM dan metode LSB dapat dilihat pada Tabel 1.

Tabel 1. Hasil Implementasi Algoritma ACM dan LSB pada Citra RGB

Citra Asli	Ukuran Citra	Citra Enkripsi	Citra Wadah	Citra Ekstraksi	Citra Dekripsi
	100x100				
	200x200				
	300x300				

DOI: https://doi.org/10.61124/sinta.v2i2.45

	400x400				
	500x500				

C. Hasil Perhitungan MSE dan PSNR

Pada perhitungan nilai MSE dan PSNR diperoleh dari perbandingan antara dua buah citra yang bertujuan untuk mengetahui kualitas dari citra tersebut setelah dilakukan dua kali pengamanan data. Citra pertama merupakan citra asli yang belum dilakukan enkripsi (penerapan algoritma ACM) dan penyisipan kedalam citra wadah (penerapan metode LSB), citra kedua adalah citra dekripsi yang sudah melalui proses ekstraksi dari penyisipan. Semua citra (25 sampel) memberikan hasil yang sama sehingga hanya ditampilkan hasil dari lima sampel yang mewakili masing-masing ukuran yang dapat dilihat pada Tabel 2.

Tabel 2. Hasil Perhitungan MSE dan PSNR

Ukuran Citra (pixel)	MSE	PSNR (dB)
100x100	0	inf
200x200	0	inf
300x300	0	inf
400x400	0	inf
500x500	0	inf

Perhitungan nilai MSE dan PSNR juga dilakukan pada citra wadah sebagai tempat untuk menyisipkan citra terenkripsi. Hasilnya disajikan dalam bentuk nilai rata-rata yang dapat dilihat pada Tabel 3.

Tabel 2. Hasil Perhitungan MSE dan PSNR Citra Wadah

Ukuran Citra (pixel)	MSE	PSNR (dB)
100x100	0.002	173.346
200x200	0.008	159.540
300x300	0.017	151.340
400x400	0.031	145.525
500x500	0.049	140,993

Penelitian ini juga memberikan rata-rata waktu pemrosesan citra dari enkripsi, penyisipan citra enkripsi kedalam citra wadah, ekstraksi (proses mendapatkan kembali citra terenkripsi dari citra wadah) sampai dekripsi yang dapat dilihat pada Tabel 3.

Tabel 2. Waktu Pemrosesan Citra

Ukuran Citra (pixel)	Waktu Pemrosesan (detik)
100x100	22,601
200x200	77,147
300x300	169,914
400x400	304,436
500x500	474,200

DOI: https://doi.org/10.61124/sinta.v2i2.45

4. DISKUSI

Berdasarkan hasil yang diperoleh pada Tabel 1. Secara visual dapat dikatakan algoritma ACM dan metode LSB berhasil diimplementasikan untuk keamanan data, hal ini dibuktikan secara visual dimana tidak terlihat ada perbedaan yang signifikan antara citra asli dengan citra dekripsi, serta citra wadah yang terlihat normal padahal citra tersebut telah disisipkan citra terenkripsi. Tabel 2. menunjukkan hasil pengujian pada citra wadah, nilai MSE dan PSNR pada citra wadah dipengaruhi oleh ukuran citra yang disisipkan. Pada penelitian ini hanya menggunakan satu ukuran untuk citra wadah, masing-masing citra enkripsi dalam berbagai ukuran disisipkan hanya pada sebuah citra wadah yang sama. Hasilnya sesuai secara teori yang menyatakan bahwa semakin kecil nilai MSE maka semakin besar nilai PSNR. Tabel 3. menunjukkan waktu pemrosesan yang berbanding lurus dimana jika ukuran citra semakin besar maka waktu pemrosesan juga semakin lama, selain itu juga bergantung pada spesifikasi perangkat yang digunakan.

5. KESIMPULAN

Keamanan informasi di dunia digital sangatlah penting, terutama dengan semakin banyaknya data yang dipertukarkan secara daring. Kriptografi dan steganografi merupakan dua teknik yang sering digunakan untuk melindungi data. Kriptografi bertujuan untuk mengubah data ke dalam bentuk yang tidak dapat diakses oleh pihak yang tidak berwenang, sedangkan steganografi berfokus pada penyembunyian data ke dalam bentuk lain, sehingga tidak dapat dideteksi oleh pihak lain.

ACM merupakan teknik kriptografi yang menggunakan transformasi geometri untuk mengenkripsi citra. Teknik ini terbukti efektif dalam menghasilkan citra yang sulit dikenali akibat enkripsi. Di sisi lain, metode LSB merupakan teknik steganografi yang menyembunyikan informasi pada bit terakhir setiap piksel citra. Metode ini dipilih karena mudah diimplementasikan dan memiliki kemampuan penyembunyian data yang baik tanpa mengubah kualitas citra.

Penerapan ACM dan LSB berbasis GUI Matlab, selain menjamin keamanan data (citra), juga dapat memberikan kemudahan bagi pengguna untuk melakukan enkripsi, penyembunyian, dan ekstraksi untuk mendapatkan kembali citra yang sama seperti citra aslinya. Hasil penelitian ini dapat memberikan kontribusi terhadap informasi yang memerlukan tingkat keamanan ekstra dan penelitian lebih lanjut terkait waktu pemrosesan dengan penggunaan perangkat yang mumpuni.

UCAPAN TERIMA KASIH

Ucapan terimakasih disampaikan kepada pembimbing dan penguji dari Prodi Teknik Elektro, Fakultas Sains dan Teknik, Universitas Nusa Cendana yang telah memberikan kontribusi terhadap penulisan artikel ilmiah ini dengan baik.

DAFTAR PUSTAKA

[1] S. Tena, B. J. Mooy, and S. I. Pella, "Implementasi Algoritma Rivest Code 6 (Rc6) Dan Steganografi Least Significant Bit (Lsb) Untuk Keamanan Data Citra Digital," *J. Media Elektro*, vol. VIII, no. 2, pp. 110–116, 2019, doi: 10.35508/jme.v0i0.1837.

[2] J. Al-Azzeh, Z. Alqadi, B. Ayyoub, and A. Sharadqh, "Improving the security of lsb image steganography," *Int. J. Informatics Vis.*, vol. 3, no. 4, pp. 384–387, 2019, doi: 10.30630/joiv.3.4.233.

[3] H. A. Atee, R. Ahmad, and N. M. Noor, "Combining Cryptography and Steganography for Data Hiding in Images," *Conf. Appl. Comput. Appl. Comput. Sci.*, vol. 5, no. 12, pp. 128–134, 2014.

[4] J. B. Eseyin and K. A. Gbolagade, "A Residue Number System Based Data Hiding Using Steganography and Cryptography," vol. 5, no. 2, pp. 345–351, 2019.

[5] S. Y. Doo, S. Tena, and V. M. Ndolu, "Implementasi Pengamanan Data Menggunakan Metode Kriptografi Hill Cipher Dan Steganografi Least Significant Bit (Lsb) Pada Media Citra Digital," *J. Media Elektro*, vol. VIII, no. 2, pp. 93–99, 2019, doi: 10.35508/jme.v0i0.1778.

[6] N. A. Setiyanto, E. H. Rachmawanto, and D. R. I. M. Setiadi, "Pengacakan Citra Digital Berwarna Dengan Kriptografi Arnold Cat Map (Acm)," in *Prosiding SNST*, 2018.

[7] R. Purba, A. Halim, and I. Syahputra, "Enkripsi Citra Digital Menggunakan Logistic Map," vol. 15, no. 2, pp. 61–71, 2014.