BAB I
PENDAHULUAN

1.1. Latar Belakang

Di era digital saat ini, pengamanan data citra semakin penting di berbagai bidang seperti kedokteran, komunikasi militer, dan analisis forensik. Citra digital memiliki korelasi piksel yang tinggi dan ukuran data yang besar, sehingga teknik enkripsi konvensional kurang efektif ketika diterapkan pada struktur citra (Zhang dkk., 2025). Penelitian terbaru juga menekankan bahwa algoritma enkripsi klasik seringkali gagal menyediakan proses *confusion–diffusion* yang memadai, terutama ketika menghadapi serangan statistik pada citra digital (Jiang & Yang, 2023). Studi lain juga melaporkan bahwa metode tradisional kurang memiliki ketahanan yang memadai terhadap teknik kriptanalisis modern, sehingga mendorong penggunaan model enkripsi yang lebih canggih (Li, 2024).

Metode *chaos-based* telah menarik perhatian yang cukup besar *chaos system* menunjukkan sifat nonlinier, ketidakpastian, dan sensitivitas terhadap kondisi awal, sehingga cocok untuk mekanisme enkripsi yang aman (Yang dkk., 2023). Beberapa penelitian menyoroti bahwa *chaos* map dapat menghasilkan keacakan yang kuat dan sifat difusi kompleks yang dibutuhkan untuk perlindungan citra yang tangguh (Sneha dkk., 2020). Tinjauan terhadap perkembangan terkini lebih lanjut menunjukkan bahwa *chaos system* secara konsisten mengungguli model klasik dalam menahan serangan korelasi dan diferensial (Dinu & Frunzete, 2025). Studi tambahan melaporkan bahwa mekanisme hibrida chaotic–fuzzy dapat lebih meningkatkan sensitivitas kunci dan kekuatan statistik, menunjukkan potensinya untuk aplikasi enkripsi citra (Mfungo dkk., 2023).

Di antara berbagai *chaos algorithm*, Modified Arnold's Cat Map (ACM) banyak digunakan sebagai teknik *confusion* karena secara efektif mengganggu hubungan spasial dan struktur geometris dalam citra (Arham & Lestari, 2023). Selain ACM tradisional, beberapa modifikasi juga telah diperkenalkan oleh peneliti lain. Modified Arnold's Cat Map merupakan pengembangan dari Modified Arnold's Cat Map konvensional dengan melakukan modifikasi parameter transformasi serta penambahan bit kunci untuk meningkatkan keamanan enkripsi citra. Metode ini

biasanya dikombinasikan dengan algoritma kriptografi seperti AES dan tahap praproses citra sehingga mampu meningkatkan kompleksitas enkripsi serta menurunkan korelasi antara citra asli dan citra terenkripsi (Shalaby dkk., 2020). Sementara itu, Modified Henon Map memainkan peran penting dalam difusi karena dinamika nonliniernya, memungkinkan modifikasi nilai piksel yang kuat di seluruh citra (Rathore & Pal, 2021). Dalam beberapa penelitian, Hénon Map dimodifikasi untuk meningkatkan keamanan enkripsi melalui dua tahap utama, yaitu *confusion* dan *diffusion*. Pada tahap *confusion*, posisi piksel citra diacak untuk mengurangi korelasi antar piksel, sedangkan pada tahap *diffusion* nilai intensitas piksel diubah menggunakan urutan chaos yang dihasilkan oleh Hénon Map. Kombinasi kedua proses ini mampu meningkatkan kompleksitas sistem enkripsi serta menghasilkan citra terenkripsi dengan distribusi piksel yang lebih acak dan tingkat keamanan yang lebih tinggi (Afifi, 2019). Penelitian terbaru menunjukkan bahwa operasi difusi berbasis Henon dapat secara signifikan meningkatkan ketidakpastian citra terenkripsi (Sudheesh dkk., 2025). Studi yang menggabungkan ACM dan Henon juga menunjukkan bahwa penerapan permutasi sebelum difusi meningkatkan keseragaman histogram dan mengurangi korelasi piksel (Ratna dkk., 2021). Metode hibrida yang lebih canggih telah diusulkan, termasuk integrasi *chaos* map dengan teknik optimasi untuk menyempurnakan urutan permutasi (Abed & Al-Jawher, 2024). Arsitektur berlapis *multi-chaotic* juga telah terbukti meningkatkan kompleksitas dan meningkatkan ketahanan statistik pada gambar terenkripsi (Musthofa dkk., 2025). Selain itu, model enkripsi citra berwarna berdasarkan ACM dan Henon menunjukkan peningkatan kinerja dalam menjaga keacakan dan degradasi visual (Nurul dkk., 2024).

Terlepas dari kemajuan ini, beberapa kesenjangan penelitian masih tetap ada. Meskipun algoritma hibrida dan *multi-chaotic* telah banyak dieksplorasi, hanya sedikit penelitian yang secara langsung membandingkan urutan berbeda dari *chaos* map yang sama, seperti ACM - Henon dan Henon – ACM (Es-Sabry dkk., 2022), (Zia dkk., 2022). Penelitian yang dilakukan oleh (Irawan & Rachmawanto, 2022) mengenai implementasi algoritma Arnold's Cat Map dan Hénon Map telah menunjukkan bahwa kedua metode tersebut mampu melakukan proses enkripsi dan

dekripsi citra dengan baik. Namun demikian, penelitian tersebut masih memiliki beberapa keterbatasan. Pengujian yang dilakukan masih terbatas pada sejumlah citra uji dengan karakteristik tertentu dan belum mengevaluasi performa algoritma terhadap variasi citra yang lebih beragam baik dari segi format maupun kompleksitas tekstur. Selain itu, analisis keamanan yang dilakukan masih berfokus pada parameter statistik seperti korelasi piksel, *differential attack* (NPCR dan UACI), serta kualitas citra menggunakan PSNR, sehingga belum mencakup analisis keamanan yang lebih mendalam seperti analisis ruang kunci (*key space analysis*), ketahanan terhadap serangan *brute force*, maupun evaluasi kinerja komputasi seperti waktu proses enkripsi dan dekripsi. Oleh karena itu, diperlukan penelitian lanjutan yang tidak hanya mengevaluasi kualitas enkripsi dari sisi statistik, tetapi juga mempertimbangkan aspek keamanan yang lebih komprehensif serta performa algoritma dalam berbagai kondisi citra digital. Penelitian yang dikemukakan oleh (Sheela dkk., 2018) membahas penggunaan modified Hénon map sebagai metode chaos untuk enkripsi citra digital guna mengatasi kelemahan algoritma konvensional dalam menangani data citra yang besar dan berkorelasi tinggi. Modifikasi dilakukan dengan mengganti komponen nonlinier pada Hénon map sehingga menghasilkan rentang chaos yang lebih luas (meningkat dari sekitar 7% menjadi 56%), yang berdampak pada peningkatan keamanan sistem. Hasil pengujian menunjukkan bahwa algoritma enkripsi yang diusulkan mampu menghasilkan distribusi piksel yang acak, korelasi antar piksel yang sangat rendah, serta nilai NPCR, UACI, dan entropy yang mendekati nilai ideal. Hal ini menandakan bahwa metode tersebut memiliki tingkat keacakan dan ketahanan yang tinggi terhadap berbagai serangan kriptografi, sehingga efektif dan layak digunakan untuk pengamanan citra digital. Penelitian yang dilakukan oleh (Shalaby dkk., 2020) menggunakan metode enkripsi citra medis berbasis gabungan chaos dan kriptografi yang disebut ECAT-AES-131, yaitu pengembangan dari Arnold's Cat Map yang dikombinasikan dengan algoritma AES. Metode ini diawali dengan tahap preprocessing menggunakan Butterworth High Pass Filter untuk mempertajam detail citra medis agar tidak hilang selama proses enkripsi. Selanjutnya, dilakukan pengacakan posisi piksel menggunakan modified Arnold's Cat Map, kemudian

hasilnya dienkripsi menggunakan AES dengan penambahan 3 bit kunci (dari 128 menjadi 131 bit) untuk meningkatkan keamanan tanpa menambah beban komputasi secara signifikan. Hasil penelitian menunjukkan bahwa metode yang diusulkan memiliki performa lebih baik dibandingkan AES standar maupun kombinasi Cat Map-AES. Hal ini dibuktikan dengan nilai korelasi yang lebih rendah (mendekati nol), serta nilai NPCR dan UACI yang lebih tinggi, yang menunjukkan perubahan signifikan pada citra terenkripsi sehingga lebih tahan terhadap serangan diferensial. Selain itu, kualitas citra hasil dekripsi tetap terjaga dengan baik (ditunjukkan oleh PSNR), sehingga informasi medis tidak rusak. Secara keseluruhan, metode ini efektif dalam meningkatkan keamanan sekaligus menjaga kualitas citra medis dengan efisiensi komputasi yang baik. Selain itu, banyak jurnal yang berfokus pada domain citra tertentu seperti citra medis, citra domain yang terkompresi, atau kumpulan data skala abu-abu, menimbulkan ketidakpastian mengenai konsistensi di berbagai format termasuk JPG, PNG, BMP, WEBP, dan TIFF (Tiwari dkk., 2025), (Kanwal dkk., 2024). Model lain, seperti 3D *chaotic encryptors*, telah diusulkan tetapi jarang dibandingkan dengan kombinasi dua peta yang lebih ringan seperti ACM dan Henon (Lu dkk., 2025). Beberapa studi juga menyoroti bahwa evaluasi kinerja sering kali mengabaikan metrik penting seperti Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Avalanche Effect (AE), Mean Squre Error (MSE), Peak Signal to Noise Ratio (PSNR) dan analisis korelasi di seluruh kumpulan data multi-format (Ibrahim & Venkatesan, 2025). Selain itu, model enkripsi citra terkompresi telah memperkenalkan dimensi *chaos* baru, tetapi penerapannya pada format citra umum masih belum pasti (Tiwari dkk., 2025).

Meskipun banyak metode enkripsi citra berbasis *chaos* telah diusulkan, alasan pemilihan *chaos* map tertentu dan dampak urutan kombinasinya tidak selalu dijelaskan dengan jelas. Modified Arnold's Cat Map banyak digunakan untuk permutasi piksel guna mengurangi korelasi spasial, sedangkan Modified Henon Map umumnya diadopsi untuk difusi nilai piksel karena sensitivitasnya yang kuat terhadap kondisi awal (Hosny dkk., 2024), (Alkhonaini dkk., 2024), (Vinoth Raj dkk., 2025). Namun, efektivitas penggunaan peta-peta ini secara individual dibandingkan dengan kombinasinya, serta pengaruh penerapan difusi sebelum atau

setelah permutasi, belum dievaluasi secara sistematis (Subathra & Thanikaiselvan, 2025), (Darani dkk., 2024). Studi ini mengatasi kesenjangan tersebut dengan penggabungan metode Modified ACM dan Modifed Henon Map berdasarkan kinerja enkripsi visual dan statistik.

1.2. Tujuan Penelitian

Penelitian ini bertujuan untuk mengevaluasi kualitas enkripsi citra digital menggunakan Modified Arnold's Cat Map dan Modified Henon Map, yang diimplementasikan secara individual dan dalam dua urutan kombinasi. Dengan mengetahui dari berbagai format citra dan memberikan evaluasi kuantitatif yang komprehensif, penelitian ini berupaya menentukan konfigurasi *chaos* yang optimal untuk mencapai keamanan statistik yang kuat, kemampuan difusi yang tinggi, dan peningkatan keacakan pada data citra terenkripsi.

1.3. Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini yaitu dapat memberikan kontribusi dalam pengembangan teknik enkripsi citra digital berbasis chaos dengan tingkat keamanan yang lebih tinggi. Selain itu, evaluasi kualitas enkripsi yang dilakukan akan menjadi referensi penting bagi peneliti lain dalam memilih metode enkripsi yang efektif untuk melindungi data citra. Hasil penelitian ini juga dapat memperkaya literatur terkait penggunaan kombinasi algoritma Modified Arnold's Cat Map dan Modified Modified Henon Map dalam bidang keamanan informasi.