Journal of Applied Informatics and Computing (JAIC)
Vol.9, No.4, August 2025, pp. 1280~1289
e-ISSN: 2548-6861

Layered Image Encryption Method Based on Combination of Logistic Map, Henon Map, and Sine Map to Enhance Digital Image Security

Amir Musthofa [1]*, De Rosal Ignatius Moses Setiadi [2]*
* Teknik Informatika, Universitas Dian Nuswantoro
amirmusthofa321@gmail.com [1], moses@dsn.dinus.ac.id [2]

Article Info

Article history:

Received 2025-04-30
Revised 2025-06-02
Accepted 2025-07-03

Keyword:

Chaos Encryption,
Logistic Map,
Henon Map,
Sine Map,
Image Security.

ABSTRACT

In today's digital era, ensuring the confidentiality of image data is crucial due to the widespread use of images in fields such as medical imaging, military communication, and multimedia applications. This study proposes a layered image encryption method by integrating three chaotic systems: Logistic Map, Henon Map, and Sine Map. Each layer in the encryption process applies a different chaotic map to sequentially perform pixel permutation, XOR-based substitution, and modulus-based substitution. Key generation is carried out by producing pseudo-random number sequences derived from the iterations of each chaotic map: the Logistic Map (using specific initial and control parameters), the Henon Map (with two initial condition variables), and the Sine Map (based on a sine function), all of which are highly sensitive to initial conditions and control parameters. These sequences are then used as keys in each encryption stage. The proposed method strengthens the principles of confusion and diffusion, thereby enhancing the security and randomness of the encrypted images. Evaluation was conducted using metrics such as histogram analysis, entropy, chi-square, correlation coefficient, PSNR, and BER. The experimental results demonstrate that the method produces encrypted images with strong statistical characteristics and high resilience against common cryptographic attacks. Thus, this approach makes a significant contribution to the development of secure and efficient image encryption techniques based on chaos theory.

I. PENDAHULUAN

Di era digital, keamanan informasi telah menjadi perhatian utama, terutama dengan meningkatnya ketergantungan pada komunikasi digital dan penyimpanan data [1], [2]. Enkripsi adalah salah satu teknik penting yang digunakan untuk melindungi informasi sensitif dari akses yang tidak sah [3]. Oleh karena itu, perkembangan metode enkripsi menjadi sangat krusial, terutama karena selalu terjadi perlombaan antara pembuat sistem keamanan dan para cryptanalyst yang berusaha membongkarnya. Jika metode enkripsi tidak terus diperbarui dan diperkuat, maka informasi yang dilindungi berisiko terekspos oleh teknik cryptanalysis yang semakin canggih [4]. Secara umum, berbagai jenis data digital dapat dienkripsi, seperti teks, dokumen, file audio, video, maupun gambar. Setiap jenis data memiliki karakteristik unik yang memengaruhi pendekatan enkripsi yang digunakan. Dalam konteks ini, gambar menjadi salah satu bentuk data yang menarik untuk dienkripsi karena menawarkan tantangan yang lebih kompleks dibandingkan data teks [5], [6]. Tantangan utama dalam enkripsi gambar terletak pada sifat dasar dari struktur pikselnya. Pada umumnya, piksel dalam sebuah gambar digital memiliki tingkat korelasi yang sangat tinggi, terutama antara piksel-piksel yang berdekatan. Korelasi ini membentuk pola visual yang konsisten, dan jika tidak diacak dengan baik, dapat dimanfaatkan oleh pihak yang tidak berwenang untuk menebak isi gambar meskipun sudah dienkripsi. Oleh karena itu, enkripsi gambar harus mampu menghancurkan korelasi antar piksel agar informasi visual asli tidak bisa direkonstruksi tanpa kunci yang sah. Mengingat pentingnya gambar dalam berbagai bidang, seperti pencitraan medis, komunikasi militer, dan aplikasi multimedia, tantangan dalam menjaga kerahasiaannya menjadi semakin besar. Dalam

bidang-bidang tersebut, memastikan kerahasiaan dan integritas gambar sangatlah krusial, karena kebocoran atau manipulasi gambar dapat berisiko merusak data atau merugikan pihak-pihak terkait. Dengan demikian, pengembangan metode enkripsi yang efektif untuk gambar tidak hanya menjadi tantangan teknis, tetapi juga aspek penting dalam menjaga keamanan informasi digital di era modern ini [5], [6], [7]. Metode enkripsi tradisional, meskipun efektif untuk data teks, seringkali kurang memadai ketika diterapkan pada gambar karena karakteristik uniknya, seperti redundansi yang tinggi dan ukuran data yang besar. Oleh karena itu, para peneliti beralih ke teknik yang lebih canggih, termasuk enkripsi berbasis chaos, untuk mengatasi tantangan ini [8], [9], [10].

Teori chaos, dengan sifat-sifat inherentnya seperti sensitivitas terhadap kondisi awal, ketidakpastian, dan ergodisitas, telah muncul sebagai pendekatan yang menjanjikan untuk enkripsi gambar [11]. Sistem chaos, seperti Logistic Map, Henon Map, dan Sine Map, sangat cocok untuk aplikasi kriptografi karena kemampuannya menghasilkan urutan pseudo-acak yang sangat sensitif terhadap kondisi awal. Sifat-sifat ini membuat sistem chaos ideal untuk menciptakan algoritma enkripsi yang aman dan efisien [9].

Logistic Map adalah sistem chaos yang terkenal yang menggambarkan pertumbuhan populasi dalam ekologi. Dalam konteks enkripsi, sistem ini digunakan untuk menghasilkan urutan chaos yang dapat digunakan untuk mengacak posisi piksel dalam gambar. Kesederhanaan Logistic Map dan sensitivitasnya yang tinggi terhadap kondisi awal menjadikannya pilihan populer untuk skema enkripsi berbasis chaos. Ketika parameter kontrol tertentu dipilih, sistem ini menunjukkan perilaku chaos yang sangat sensitif terhadap perubahan kecil pada kondisi awal, sehingga meningkatkan keamanan enkripsi [9], [12].

Henon Map, di sisi lain, adalah sistem dinamika diskrit dua dimensi yang pertama kali diperkenalkan oleh Michel Henon pada tahun 1976. Sistem ini sering digunakan dalam enkripsi gambar karena perilaku chaos yang kompleks dan sensitivitasnya terhadap parameter awal. Henon Map sangat efektif dalam proses permutasi dan substitusi dalam enkripsi gambar karena kemampuannya menghasilkan urutan yang sangat acak dan sulit diprediksi [13], [14].

Sine Map adalah sistem chaos lain yang berbasis fungsi trigonometri sinus. Sistem ini digunakan dalam berbagai aplikasi kriptografi karena kemampuannya menghasilkan urutan angka yang memiliki sifat chaos yang kuat. Sine Map menunjukkan perilaku chaos ketika parameter kontrol berada dalam rentang tertentu, dan sering digunakan dalam proses substitusi dan modulus dalam enkripsi gambar, karena kemampuannya menghasilkan urutan yang sangat acak dan sulit diprediksi [15], [16].

Dalam penelitian ini, kami mengusulkan metode enkripsi gambar baru yang mengintegrasikan Logistic Map, Henon Map, dan Sine Map untuk menciptakan skema enkripsi berlapis. Pendekatan tiga lapisan ini dirancang untuk mengimplementasikan prinsip confusion dan diffusion secara berurutan dan saling melengkapi. Lapisan permutasi berbasis Logistic Map mengacak posisi piksel untuk menghancurkan korelasi spasial antar piksel bertetangga, sesuai prinsip difusi spasial yang dianjurkan dalam enkripsi citra [16], [17]. Lapisan XOR substitution menggunakan Henon Map untuk mengganggu distribusi nilai intensitas global, meningkatkan kerandoman dan efektivitas confusion [18]. Terakhir, substitusi modulus dari Sine Map memperkenalkan non-linearitas tambahan, yang menurut penelitian dapat memperkuat efek avalanche dan difusi lokal pada data piksel [19]. Kombinasi ketiganya menciptakan ciphertext dengan distribusi statistik yang lebih merata dan ketahanan tinggi terhadap analisis statistik dan serangan kriptografi umum.

Kontribusi utama penelitian ini adalah sebagai berikut:

1) *Skema Enkripsi Berlapis Dikembangkan:* Penelitian ini memperkenalkan skema enkripsi tiga lapis yang mengintegrasikan tiga peta chaos berbeda, yaitu Logistic Map, Henon Map, dan Sine Map, yang masing-masing digunakan secara terpisah untuk permutasi, subtitusi XOR, dan subtitusi modulus. Desain ini tidak hanya memperkaya proses *confusion* dan *diffusion* secara bertahap, tetapi juga menawarkan struktur berlapis yang belum umum dijumpai dalam literatur enkripsi berbasis chaos, menjadikannya pendekatan yang inovatif dan kompleks terhadap pengamanan citra digital.
2) *Mekanisme Pembuatan Kunci Diusulkan:* Mekanisme pembuatan kunci yang memanfaatkan sifat chaos dari Logistic Map, Henon Map, dan Sine Map diusulkan untuk menghasilkan urutan pseudo-random. Urutan ini sangat penting dalam proses enkripsi, karena kunci enkripsi menjadi sangat sensitif terhadap kondisi awal dan sulit diprediksi.
3) *Analisa Keamanan Dilakukan:* Analisa keamanan yang komprehensif dilakukan untuk mengevaluasi efektivitas metode enkripsi yang diusulkan. Analisis ini mencakup berbagai metrik, seperti analisis histogram, entropi, uji chi-square, koefisien korelasi, PSNR (Peak Signal-to-Noise Ratio), dan BER (Bit Error Rate). Metrik-metrik ini memberikan penilaian menyeluruh tentang ketahanan skema enkripsi, serta ketahanannya terhadap serangan kriptografi umum dan kemampuannya dalam menjaga integritas dan kerahasiaan gambar yang dienkripsi.

Dengan memanfaatkan sifat chaos dari Logistic Map, Henon Map, dan Sine Map, penelitian ini bertujuan untuk berkontribusi pada pengembangan teknik enkripsi gambar yang lebih aman dan efisien, memenuhi kebutuhan yang semakin meningkat akan keamanan informasi yang kuat di era digital.

II. METODE

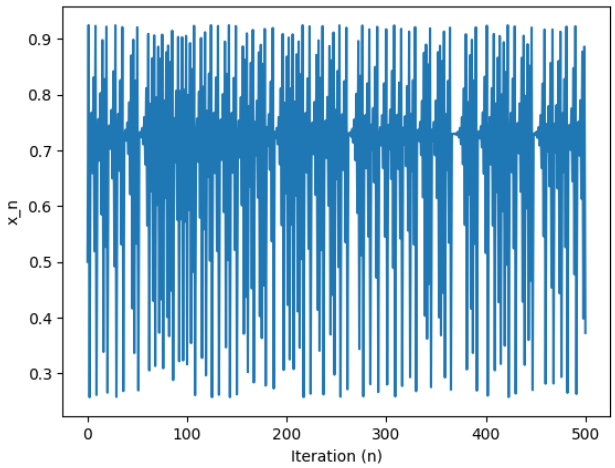
A. Logistic Map

Logistic map adalah fungsi matematis yang digunakan untuk menggambarkan pertumbuhan populasi dalam ekologi atau dinamika sistem. Namun, dalam konteks enkripsi, Logistic map digunakan sebagai fungsi chaos (kacau) yang dapat menghasilkan urutan angka yang tampaknya acak tetapi

sebenarnya dapat diprediksi jika parameter awalnya diketahui [20]. Adapun bentuk logistic map yang digunakan pada penelitian ini dapat di lihat pada (Equation 1).

$$x_{n+1} = r \times x_n(1 - x_n) \quad (1)$$

Dimana $x0$ adalah kondisi awal, kontrol parameter $r \in [0,4]$, dan $x \in [0,1]$.



Gambar 1. Logistic Map Attractor (r=3.7, x0=0.5)

Peta logistik menunjukkan perilaku chaotik ketika $r > 3{,}7$. Dalam rentang ini, sistem menjadi sangat sensitif terhadap kondisi awal, yang merupakan ciri khas sistem chaotik. Perubahan kecil pada nilai awal $x0$ dapat menyebabkan hasil yang sangat berbeda setelah beberapa iterasi, sehingga menekankan pentingnya ketelitian dalam menentukan kondisi awal saat menganalisis sistem ini.

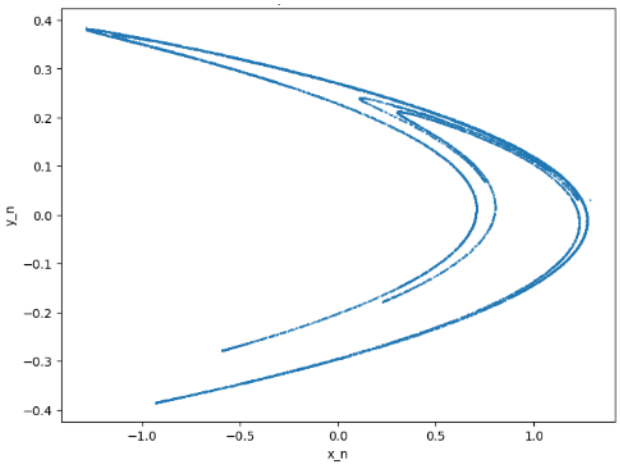
B. Henon Map

Henon Map adalah sebuah sistem dinamis diskrit yang digunakan dalam teori chaos dan sering digunakan dalam penelitian enkripsi gambar karena sifat kekacauan dan sensitivitas terhadap kondisi awalnya. Henon Map pertama kali diperkenalkan oleh matematikawan Michel Henon pada tahun 1976 sebagai model untuk menggambarkan perilaku dinamis dalam sistem fisik yang sederhana [21]. Adapun bentuk henon map yang digunakan pada penelitian ini dapat di lihat pada (Equation 2).

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \quad (2)$$

Perilaku kuat dari sistem chaos tergantung pada nilai parameter a, b yang disebut sebagai parameter kontrol. Parameter dan kondisi dari peta henon adalah sebagai berikut:

1. x_0, dimana x_0 adalah nilai awal.
2. $a \in [0,1]$, dimana a adalah parameter kontrol.
3. $K_1 = (a, x_0)$ adalah kunci rahasia dari fase permutasi.



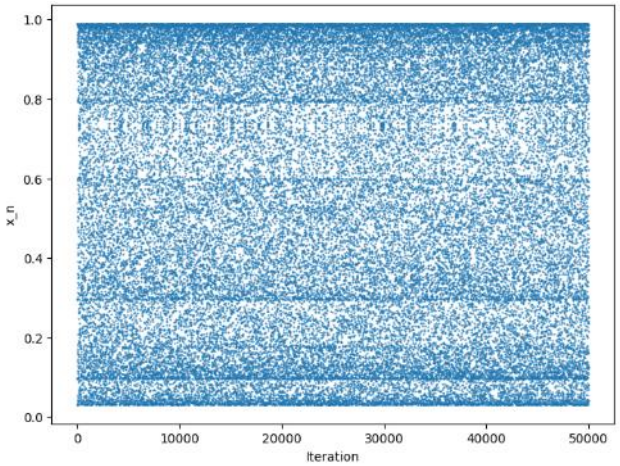
Gambar 2. Henon Map Attractor (a=1.4, b=0.3)

C. Sine Map

Sine map adalah jenis peta atau sistem dinamis yang digunakan dalam berbagai aplikasi, termasuk dalam kriptografi untuk enkripsi. Sine map bekerja berdasarkan fungsi trigonometri sinus. Peta ini beroperasi pada interval tertentu dan menghasilkan urutan angka yang memiliki sifat chaos, yang membuatnya cocok untuk digunakan dalam proses enkripsi [22]. Adapun bentuk sine map yang digunakan pada penelitian ini dapat di lihat pada (Equation 3).

$$x_{n+1} = \sin(\pi x_n) \quad (3)$$

Dimana parameter $s \in [0,1]$. Sine map chaos ketika $s \in [0.87,1]$

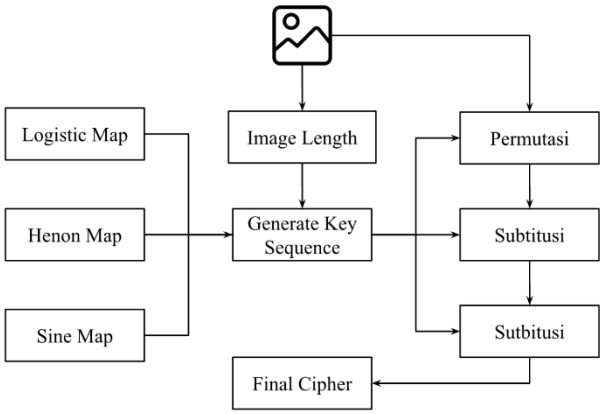


Gambar 3. Sine Map Attractor (r=0.99, x0=0.5)

D. Proposed Encryption

Pada bagian ini, kami memperkenalkan metode enkripsi gambar yang kami usulkan. Pendekatan yang dipilih menekankan teknik enkripsi yang mengikuti prinsip-prinsip pengaburan dan difusi. Kami mengintegrasikan berbagai

teknik enkripsi, termasuk penggunaan Peta Logistik, Peta Henon, dan Peta Sine, untuk menciptakan solusi enkripsi gambar yang komprehensif dan efektif. Di bawah ini, kami menjelaskan secara rinci metode yang kami usulkan, termasuk prinsip dasar, algoritme langkah demi langkah, serta komponen utama yang didukung oleh diagram alir. Sebagai ilustrasi awal dari metode yang diusulkan, dapat di lihat pada Gambar 4.



Gambar 4. Proposed Encryption Method

E. Key Generation

Pada skema yang diajukan, setiap algoritma (Logistic Map, Henon Map, dan Sine Map) memiliki metode pembuatan urutan kunci (sequence generation) yang berbeda. Setiap urutan ini dihasilkan berdasarkan rumus matematis tertentu dan digunakan untuk menghasilkan angka pseudorandom yang akan dipakai dalam proses enkripsi. Tujuan dari pembuatan urutan ini adalah untuk menghasilkan angka-angka acak yang dapat mempengaruhi piksel gambar atau data lainnya. Adapun preparation dan proses nya sebagai berikut:

1. Ubah image menjadi satu dimensi untuk mencari panjang nya yang akan digunakan untuk iterasi sequence.
2. Logistic Map
   proses pembuatan urutan kunci dimulai dengan nilai awal x0 = 0.5 dan parameter kontrol r = 3.99. Setelah itu, menggunakan equation x untuk iteratif digunakan untuk menghasilkan urutan angka berikutnya. Setiap iterasi dilakukan dengan menghitung nilai baru berdasarkan nilai sebelumnya. Hasilnya adalah key sequence untuk logistic map.
3. Henon Map
   proses pembuatan urutan kunci dimulai dengan nilai awal x0 = 0.1 dan y0 = 0.3, serta parameter kontrol a = 1.4 dan b = 0.3. Iterasi dilakukan untuk menghitung nilai baru x_n dan y_n pada setiap langkah menggunakan equation x. Hasilnya adalah key sequence untuk henon map.
4. Sine Map
   Pada Sine Map, proses pembuatan urutan kunci dimulai dengan nilai awal x0 = 0.5 dan parameter kontrol r = 0.99. Iterasi dilakukan dengan menggunakan equation x. Hasil dari iterasi ini adalah urutan angka yang akan digunakan sebagai key sequence untuk sine map.

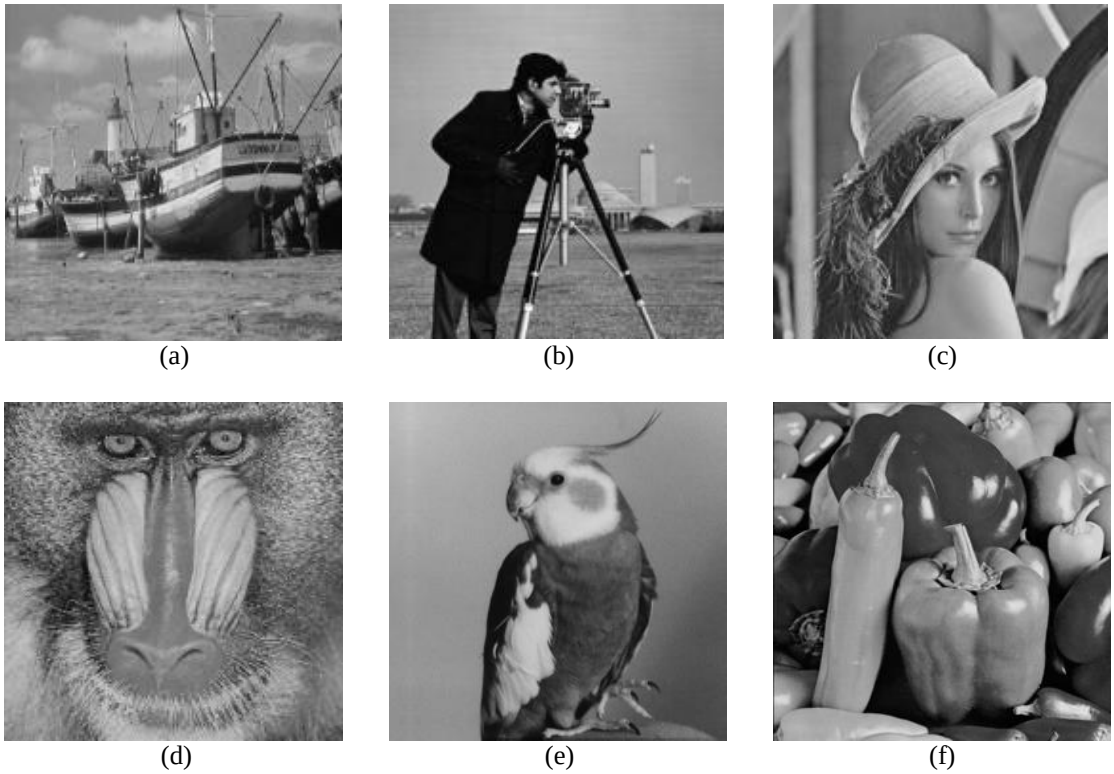
F. Encryption Proses

Dalam riset ini, teknik enkripsi yang diajukan menggunakan pendekatan 3 lapisan enkripsi, yang masing-masing lapisan menggunakan algoritma chaos, yaitu Logistic Map, Henon Map, dan Sine Map. Penjelasan lebih detail mengenai setiap lapisan akan dijabarkan berikut ini.

1. Convert gambar menjadi array 1 dimensi. Array ini digunakan untuk input multi layer encryption.
2. Lapisan Pertama, urutan kunci untuk permutasi dihasilkan dari Logistic Map, yang mengacak posisi piksel dalam gambar. Nilai awal dan parameter dari Logistic Map digunakan untuk menghasilkan urutan yang kemudian diterapkan pada gambar sebagai permutasi.
3. Lapisan Kedua, hasil dari lapisan pertama digunakan untuk proses XOR Substitution dengan urutan kunci yang dihasilkan dari Henon Map. Urutan kunci ini menghasilkan gambar yang lebih sulit dikenali.
4. Lapisan Ketiga, gambar yang telah melalui lapisan kedua kemudian dikenkripsi menggunakan Modulus Substitution dengan urutan kunci yang dihasilkan dari Sine Map, menghasilkan gambar terenkripsi yang lebih kompleks.
5. Hasil dari layer ketiga adalah final cipher, untuk proses dekripsi merupakan kebalikan dari proses enkripsi.

III. HASIL DAN PEMBAHASAN

Dalam studi ini, eksperimen dilakukan dengan memanfaatkan Python dan Google Colab sebagai platform untuk pengembangan dan pengujian. Untuk menguji efektivitas metode enkripsi yang diusulkan, beberapa gambar grayscale yang sering digunakan dalam penelitian enkripsi dipilih sebagai sampel dari situs the waterloo image repository [23]. Citra grayscale dipilih karena merepresentasikan struktur intensitas piksel yang lebih sederhada tanpa kompleksitas saluran warna (RGB), sehingga memungkinkan fokus evaluasi pada efektivitas algoritma enkripsi terhadap aspek *confusion* dan *diffusion* [24]. Selain itu, grayscale merupakan standar uji yang umum digunakan dalam penelitian enkripsi citra untuk memastikan perbandingan yang adil dengan metode terdahulu. Adapun gambar-gambar yang diuji meliputi Boat, Cameraman, Lena, Mandril, Bird, Peppers. Sebagai bagian dari evaluasi hasil enkripsi, kami menggunakan sejumlah metrik analisis, seperti analisis histogram, entropi informasi, uji chi-square, koefisien korelasi, PSNR (Peak Signal-to-Noise Ratio), BER (Bit Error Rate), dan time analysis.

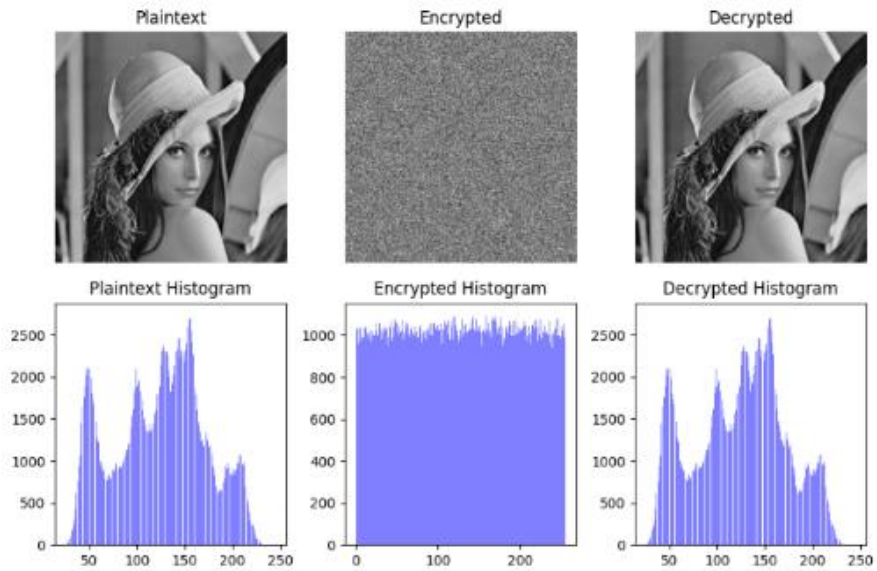


(a) (b) (c)

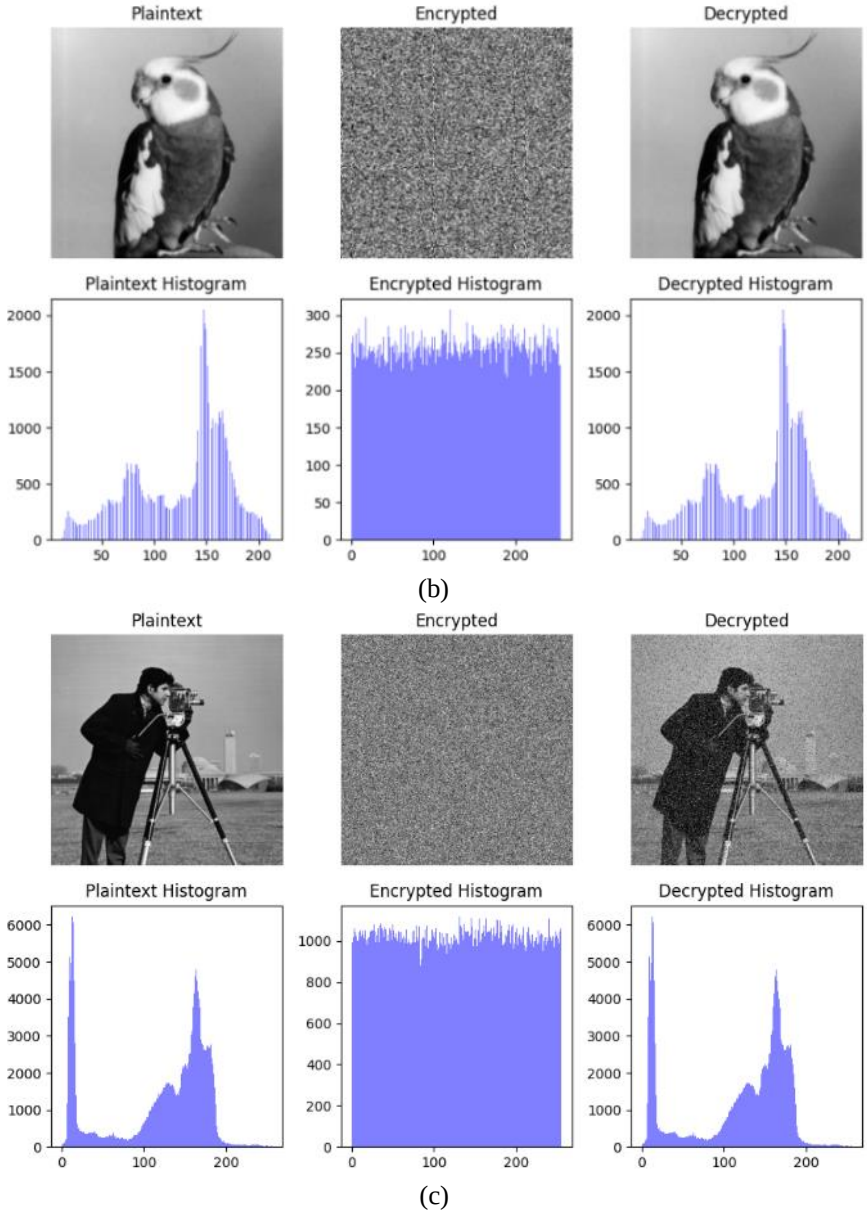
(d) (e) (f)

Gambar 5. Standart Image Used For Testing; (a) Boat, (b) Cameraman, (c) Lena, (d) Mandril, (e) Bird, (f) Peppers

A. Histogram Analysis



(a)



Gambar 6. Sample of histogram original, encrypted, decrypted image; (a) 512 image, (b) 256 image, (c) 512 attacked image

B. Entorpi Informasi

Entropi informasi adalah ukuran dari ketidakpastian atau kerandoman dalam suatu sistem atau kumpulan data. Dalam konteks pengolahan citra atau informasi, entropi mengukur seberapa banyak informasi yang dibawa oleh citra atau sinyal, atau dengansss kata lain, seberapa acak atau terstruktur data tersebut. Untuk enkripsi gambar, nilai entropi yang diharapkan adalah 8. Namun dalam praktik, mencapai nilai tepat 8 hampir tidak mungkin. Oleh karena itu, dalam evaluasi kualitas enkripsi, nilai entropi yang berada di atas atau sama dengan 7.99 dianggap sangat baik dan menunjukkan tingkat keacakan yang tinggi. Adapun bentuk matematis dari entropi informasi dapat di lihat pada (Equation 4), dan hasil perhitungan nya dapat di lihat pada Tabel 1.

$$H(X) = -\sum_{x=0}^{255} \left(\frac{H(x)}{N}\right) \log_2 \left(\frac{H(x)}{N}\right) \quad (4)$$

Dimana, *H(x)* merujuk pada jumlah piksel yang memiliki intensitas *x* dalam gambar. Sementara itu, *N* adalah total jumlah piksel dalam gambar, yang dapat dihitung dengan mengalikan dimensi gambar (panjang dan lebar). Probabilitas kemunculan intensitas piksel *x*, yang dilambangkan sebagai *p(x)*, dihitung dengan membagi jumlah piksel dengan intensitas *x* (yaitu *H(x)*) dengan total jumlah piksel dalam gambar (yaitu *N*).

TABEL I
HASIL ENTROPI INFORMASI

Image	Method [25]	Method [26]	Method [27]	Proposed
Boat	-	7.9993	-	7.9991
Cameraman	7.9975	7.9992	7.9994	7.9990
Lena	7.9974	7.9992	7.9994	7.9992
Mandril	-	7.9992	7.9994	7.9992
Bird	-	-	-	7.9973
Peppers	-	-	-	7.9973

TABEL II
HASIL CHI-SQUARE

Image	Method [28]	Method [26]	Method [27]	Proposed
Boat	-	242.3671	-	292.5937
Cameraman	221.6254	257.4765	247.1343	339.4511
Lena	191.6719	256.8320	234.4334	277.6230
Mandril	230.6719	255.214	250.2232	263.5273
Bird	-	-	-	241.6171
Peppers	-	-	-	243.6640

C. Chi-Square

Chi-square (χ^2) adalah salah satu uji statistik yang digunakan untuk menentukan apakah ada hubungan atau perbedaan yang signifikan antara variabel kategori dalam suatu dataset. Uji ini sering digunakan dalam analisis data untuk menguji hipotesis tentang distribusi frekuensi atau untuk mengevaluasi asosiasi antar variabel kategori. Untuk enkripsi gambar, nilai chi-square yang baik tidak lebih dari 293,2478. Bentuk matematis dari chi-square dapat di lihat pada (Equation 5), dan hasil perhitungan nya dapat di lihat pada Tabel 2.

$$X^2 = \sum \frac{(O-E)^2}{E} \quad (5)$$

Dimana, O adalah frekuensi yang diamati, sedangkan E adalah frekuensi yang diharapkan berdasarkan hipotesis nol.

D. Koefisien Korelasi

Koefisien Korelasi Pearson (KKP) adalah suatu ukuran statistik yang digunakan untuk mengukur sejauh mana dua variabel memiliki hubungan linier yang terarah. Ini sangat berguna untuk memahami bagaimana dua variabel terkait satu sama lain dan sejauh mana perubahannya berkorelasi secara langsung. Untuk enkripsi gambar, nilai koefisien korelasi yang ideal adalah yang mendekati angka nol. Bentuk sistematis dari koefisien korelasi dapat di lihat pada (Equation 6), dan hasil perhitungan nya dapat di lihat pada Tabel 3.

$$CC = \frac{\sum_{i=1}^{N}(X_i - \frac{1}{N}\sum_{i=1}^{N} X_i)(Y_i - \frac{1}{N}\sum_{i=1}^{N} Y_i)}{N\sigma_X\sigma_Y} \quad (6)$$

Dimana, CC adalah Koefisien Korelasi Pearson yang mengukur hubungan linier antara dua variabel, X dan Y. N adalah jumlah pasangan data X_i dan Y_i yang dianalisis. X_i dan Y_i adalah nilai variabel X dan Y pada pengamatan ke-i. σ_X dan σ_Y adalah simpangan baku dari variabel X dan Y, yang mengukur sejauh mana data tersebar dari rata-rata.

TABEL III
HASIL KOEFISIEN KORELASI

Image	Size	Direction	Method [26]	Method [25]	Method [29]	Proposed
Boat	512x512	H	-0.000331	-	0.0003	0.00150
		V	-0.000359	-	0.0034	-0.00027
		D	-0.000156	-	0.0011	0.00350
Cameraman	512x512	H	0.000657	0.00088	0.0014	-0.00157
		V	-0.000125	−0.00036	0.0002	0.00054
		D	-0.000277	−0.00064	0.0035	0.00395
Lena	512x512	H	0.000715	0.00058	0.0032	-0.00281
		V	0.000111	0.00061	0.0016	0.00119
		D	-0.00016	−0.00030	0.0023	0.00063
Mandril	512x512	H	0.000961	-	0.0029	-0.00091
		V	-0.000334	-	0.0033	-0.00090
		D	-0.000399	-	0.0062	0.00023
Peppers	256x256	H	-	-	0.0016	0.00660
		V	-	-	0.0059	-0.00323
		D	-	-	0.0034	-0.00524

E. PSNR

PSNR (Peak Signal-to-Noise Ratio) adalah metrik yang sering digunakan untuk mengukur kualitas gambar atau sinyal setelah mengalami proses kompresi, distorsi, atau pemrosesan lainnya. PSNR mengukur rasio antara kekuatan sinyal asli dengan tingkat kebisingan (noise) yang ditambahkan, dengan cara membandingkan gambar asli dan gambar yang sudah diubah. PSNR dihitung berdasarkan Mean Squared Error (MSE) antara dua gambar, yang mana semakin kecil nilai MSE, semakin baik kualitas gambar yang dihasilkan. Bentuk matematis dari PSNR dapat di lihat pada (Equation 7), dan hasil perhitungan nya dapat di lihat pada Tabel IV.

$$PSNR = 10 \times \log_{10}\left(\frac{Max\ Pixel^2}{MSE}\right) \quad (7)$$

Dimana, MSE (Mean Squared Error) mengukur rata-rata perbedaan kuadrat antara gambar asli dan gambar yang diproses, semakin kecil MSE, semakin baik kualitas gambar. Max Pixel adalah nilai piksel maksimum dalam gambar, yang untuk gambar 8-bit adalah 255. PSNR menggunakan nilai ini untuk membandingkan rasio antara sinyal (gambar asli) dan noise (distorsi gambar), dengan semakin tinggi PSNR menunjukkan kualitas gambar yang lebih baik.

TABEL IV
HASIL PSNR

Image	Method [28]	Method [30]	Proposed
Boat	-	-	27.89 dB
Cameraman	7.46 dB	29.49 dB	27.90 dB
Lena	9.17 dB	32.56 dB	27.89 dB
Mandril	8.91 dB	23.01 dB	27.90 dB
Bird	-	-	27.89 dB
Peppers	-	-	27.88 dB

F. BER

Bit Error Rate (BER) adalah metrik yang digunakan untuk mengukur jumlah bit yang salah atau berbeda antara dua representasi digital dari suatu data, seperti gambar. Dalam konteks gambar, BER sering digunakan untuk mengevaluasi tingkat keacakan ciphertext dengan membandingkannya terhadap plaintext (gambar asli). Nilai BER dihitung sebagai rasio jumlah bit yang berbeda antara dua gambar terhadap total jumlah bit secara keseluruhan.

Pada penelitian ini, perhitungan BER dilakukan dengan cara membandingkan bit demi bit antara plaintext dan ciphertext. Tujuan dari pengukuran ini adalah untuk menilai tingkat *confusion*, yaitu sejauh mana ciphertext telah kehilangan pola-pola yang ada pada plaintext. Nilai BER yang mendekati 0,5 menunjukkan bahwa separuh bit dari ciphertext berbeda dengan plaintext, yang merupakan indikator bahwa ciphertext memiliki distribusi bit yang acak dan tidak menampakkan korelasi dengan plaintext. Kondisi ini dianggap optimal dalam konteks pengamanan data, karena mengindikasikan bahwa hasil enkripsi tidak mengungkapkan struktur gambar asli.

Perlu dicatat bahwa pengujian ini tidak dimaksudkan untuk mengukur plaintext sensitivity atau efek avalanche, yang memerlukan skenario berbeda, yakni dengan membandingkan dua ciphertext yang dihasilkan dari dua plaintext yang hanya berbeda satu bit. Oleh karena itu, interpretasi nilai BER dalam konteks ini murni sebagai pengukuran tingkat keacakan relatif terhadap gambar asli. Adapun bentuk matematis dari BER dapat di lihat pada (Equation 8), dan hasil perhitungan nya dapat di lihat pada Tabel V.

$$BER = \frac{Jumlah\ Bit\ yang\ Salah}{Total\ Jumlah\ Bit} \quad (8)$$

Bit Error Rate (BER) adalah rasio jumlah bit yang salah dibandingkan dengan total jumlah bit yang ada dalam dua gambar. Semakin rendah BER, semakin kecil perbedaan antara gambar asli dan gambar yang diproses.

TABEL V
HASIL BER

Image	Color	Size	Proposed
Boat	Grayscale	512x512	0.499341
Cameraman	Grayscale	512x512	0.499866
Lena	Grayscale	512x512	0.500127
Mandril	Grayscale	512x512	0.500082
Bird	Grayscale	256x256	0.501115
Peppers	Grayscale	256x256	0.499610

G. Time Analysis

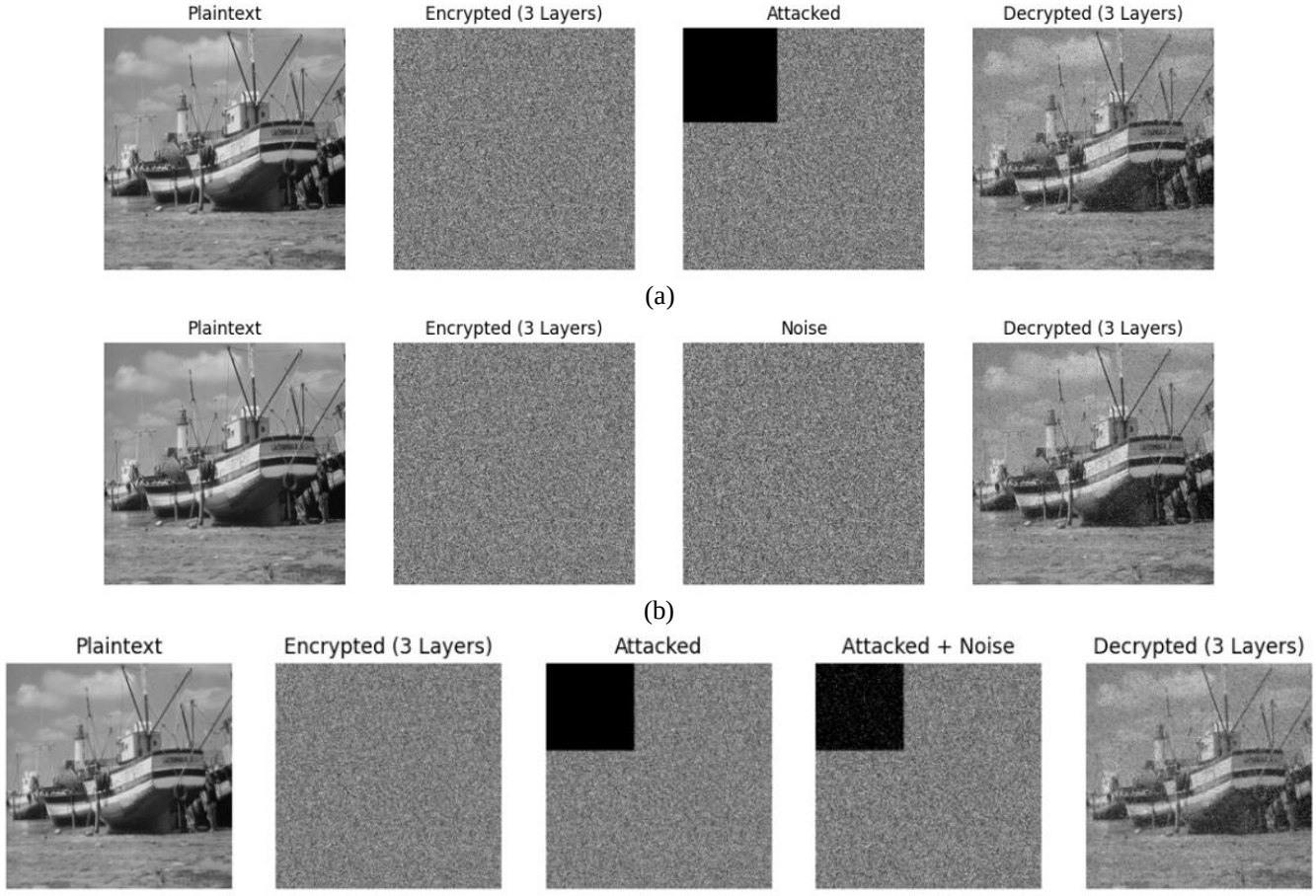
Selain aspek keamanan, efisiensi waktu eksekusi merupakan faktor penting dalam mengevaluasi kinerja algoritma enkripsi, terutama dalam aplikasi real-time dan sistem dengan keterbatasan sumber daya. Oleh karena itu, pada subbab ini dilakukan analisis terhadap waktu yang dibutuhkan untuk proses enkripsi dan dekripsi menggunakan metode yang diusulkan. Analisis waktu ini bertujuan untuk menilai kelayakan implementasi metode pada skenario praktis serta mengidentifikasi potensi optimasi yang dapat dilakukan di masa mendatang. Pengujian dilakukan pada beberapa gambar uji dengan ukuran dan kompleksitas yang seragam untuk memastikan konsistensi hasil. Lama waktu untuk enkripsi dapat di lihat pada Tabel VI.

TABEL VI
TIME ANALYSIS

Image	Size	Time (sec)
Boat	512x512	0.0334
Cameraman	512x512	0.0335
Lena	512x512	0.0352
Mandril	512x512	0.0572
Bird	256x256	0.0104
Peppers	256x256	0.0174

H. Robustness Test

Untuk mengukur ketahanan metode enkripsi yang diusulkan terhadap gangguan eksternal dan manipulasi data, dilakukan pengujian *robustness* terhadap beberapa jenis serangan umum yang mungkin terjadi dalam transmisi atau penyimpanan citra digital. Uji ketahanan ini melibatkan tiga skenario: Serangan cropping atau pemotongan sebagian area gambar, penambahan noise tipe salt and pepper yang sering muncul akibat gangguan sinyal atau kompresi, serta kombinasi dari kedua serangan tersebut.



Gambar 7. Robustnes Tes; (a) Cropping Image, (b) Noise Image, (c) Cropping + Noise Image

Hasil dari pengujian ini menunjukkan bahwa metode enkripsi yang diusulkan mampu mempertahankan integritas data citra terenkripsi dan memastikan bahwa gambar asli tetap dapat direkonstruksi secara layak setelah proses dekripsi, meskipun telah mengalami gangguan.

IV. KESIMPULAN

Penelitian ini mengusulkan metode enkripsi gambar berlapis menggunakan kombinasi tiga peta chaos, yaitu Logistic Map, Henon Map, dan Sine Map. Integrasi ketiganya memungkinkan implementasi prinsip *confusion* dan *diffusion* secara optimal, yang terbukti meningkatkan tingkat keamanan gambar terenkripsi. Hasil evaluasi menggunakan berbagai metrik seperti histogram, entropi informasi, chi-square, koefisien korelasi, PSNR, dan BER menunjukkan bahwa metode yang diusulkan mampu menghasilkan gambar terenkripsi dengan distribusi piksel yang merata, tingkat keacakan tinggi, dan ketahanan yang baik terhadap serangan kriptografi umum. Dengan demikian, pendekatan ini tidak hanya meningkatkan keamanan informasi visual, tetapi juga membuktikan bahwa kombinasi sistem chaos dapat menjadi fondasi yang kuat dalam pengembangan algoritma enkripsi gambar modern.

DAFTAR PUSTAKA

[1] R. D. Syah, S. Madenda, R. J. Suhatril, and S. Harmanto, "Digital Image Encryption using Composition of RaMSH-1 Map Transposition and Logistic Map Keystream Substitution," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, pp. 565–571, 2023, doi: 10.14569/IJACSA.2023.0140365.

[2] A. Alaa Hammad, F. Tarik Jasim, and C. Author, "Adaptive Cyber Defense using Advanced Deep Reinforcement Learning Algorithms: A Real-Time Comparative Analysis," *Journal of Computing Theories and Applications*, vol. 2, no. 4, pp. 523–535, Apr. 2025, doi: 10.62411/jcta.12560.

[3] K. A. Santoso, M. F. Fakih, and A. Kamsyakawuni, "Text Insertion and Encryption Using The Bit-Swapping Method in Digital Images," *Journal of Applied Informatics and Computing*, vol. 8, no. 1, pp. 86–90, Jul. 2024, doi: 10.30871/JAIC.V8I1.7395.

[4] A. Singh, K. B. Sivangi, and A. N. Tentu, "Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 257–272, Feb. 2024, doi: 10.62411/jcta.9851.

[5] D. B. P. Pamungkas, I. Isnawaty, and L. M. F. Aksara, "Implementation of Samba Server Using OpenVPN Based on Single Board Computer (SBC) for Private Cloud Storage," *Journal of Applied Informatics and Computing*, vol. 8, no. 2, pp. 316–325, Nov. 2024, doi: 10.30871/JAIC.V8I2.8324.

[6] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, "OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection," *Journal of Future Artificial Intelligence and Technologies*, vol. 1, no. 4, pp. 401–416, Feb. 2025, doi: 10.62411/faith.3048-3719-63.

[7] D. R. I. M. Setiadi, S. K. Ghosal, and A. K. Sahu, "AI-Powered Steganography: Advances in Image, Linguistic, and 3D Mesh Data Hiding – A Survey," *Journal of Future Artificial Intelligence and Technologies*, vol. 2, no. 1, pp. 1–23, Apr. 2025, doi: 10.62411/faith.3048-3719-76.

[8] A. Susanto *et al.*, "Triple layer image security using bit-shift, chaos, and stream encryption," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 980–987, Jun. 2020, doi: 10.11591/EEI.V9I3.2001.

[9] S. Sahid, A. Dhoruri, D. Lestari, E. R. Sari, and M. Fauzan, "Sistem Kriptografi Stream Cipher Berbasis Fungsi Chaos untuk Keamanan Informasi," *Jurnal Sains Dasar*, vol. 8, no. 1, pp. 6–12, Feb. 2019, doi: 10.21831/JSD.V8I1.38666.

[10] Z. A. N. Fauzyah, A. Sambas, P. W. Adi, and D. R. I. M. Setiadi, "Quantum Key Distribution-Assisted Image Encryption Using 7D and 2D Hyperchaotic Systems," *Journal of Future Artificial Intelligence and Technologies*, vol. 2, no. 1, pp. 47–62, Apr. 2025, doi: 10.62411/faith.3048-3719-93.

[11] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A New Algorithm for Digital Image Encryption Based on Chaos Theory," *Entropy 2021, Vol. 23, Page 341*, vol. 23, no. 3, p. 341, Mar. 2021, doi: 10.3390/E23030341.

[12] T. Gbaden and B. Nachaba, "Chaos Based Image Encryption Scheme Using One Dimensional Exponential Logistic Map," *Current Journal of Applied Science and Technology*, vol. 38, no. 6, pp. 1–14, Jan. 2020, doi: 10.9734/cjast/2019/v38i630451.

[13] A. Afifi, "A Chaotic Confusion-Diffusion Image Encryption Based On Henon Map," *International Journal of Network Security & Applications (IJNSA)*, vol. 11, no. 4, 2019, doi: 10.5121/ijnsa.2019.11402.

[14] A. A. P. Ratna *et al.*, "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion," *Advances in Science, Technology and Engineering Systems*, vol. 6, no. 1, pp. 316–326, 2021, doi: 10.25046/aj060136.

[15] X. Wang Maozhen Zhang, C. Xingyuan Wang, and M. Zhang, "High-sensitivity synchronous image encryption based on improved one-dimensional compound sine map," *IET Image Process*, vol. 15, no. 10, pp. 2247–2265, Aug. 2021, doi: 10.1049/IPR2.12193.

[16] M. A. Khan, J. Khan, A. A. Alghamdi, and S. M. A. B. Saidan, "Image Encryption Enabling Chaotic Ergodicity with Logistic and Sine Map," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, pp. 437–442, Sep. 2021, doi: 10.14569/IJACSA.2021.0120750.

[17] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, Dec. 2015, doi: 10.1016/J.NEUCOM.2014.11.095.

[18] I. A. Pikrammenos, P. Tolis, and P. Perakis, "A Chaotic Confusion-Diffusion Image Encryption Based on Henon Map," *International Journal of Network Security & Its Applications (IJNSA) Vol. 11, No.4*, vol. 11, no. 4, p. 19, Jul. 2019, doi: 10.5121/IJNSA.2019.11401.

[19] X. Wang Maozhen Zhang, C. Xingyuan Wang, and M. Zhang, "High-sensitivity synchronous image encryption based on improved one-dimensional compound sine map," *IET Image Process*, vol. 15, no. 10, pp. 2247–2265, May 2021, doi: 10.1049/IPR2.12193.

[20] E. W. Weisstein, "Logistic Map", Accessed: Apr. 29, 2025. [Online]. Available: https://mathworld.wolfram.com/LogisticMap.html

[21] M. Benedicks and L. Carleson, "The Dynamics of the Henon Map," *The Annals of Mathematics*, vol. 133, no. 1, p. 73, Jan. 1991, doi: 10.2307/2944326.

[22] J. Griffin, "The Sine Map," 2013.

[23] "Repository." Accessed: Apr. 29, 2025. [Online]. Available: https://links.uwaterloo.ca/Repository.html

[24] M. M. Hazzazi, M. U. Rehman, A. Shafique, A. Aljaedi, Z. Bassfar, and A. B. Usman, "Enhancing image security via chaotic maps, Fibonacci, Tribonacci transformations, and DWT diffusion: a robust data encryption approach," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-62260-3.

[25] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimed Tools Appl*, vol. 78, no. 15, pp. 22023–22043, Aug. 2019, doi: 10.1007/s11042-019-7453-3.

[26] M. N. E. Farandi, A. Marjuni, N. Rijati, and D. R. I. M. Setiadi, "Enhancing image encryption security through integration multi-chaotic systems and mixed pixel-bit level," *Imaging Science Journal*, 2024, doi: 10.1080/13682199.2024.2398954.

[27] D. R. I. M. Setiadi, R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, "Image Encryption using Half-Inverted Cascading Chaos Cipheration," *Journal of Computing Theories and Applications*, vol. 1, no. 2, pp. 61–77, Oct. 2023, doi: 10.33633/jcta.v1i2.9388.

[28] I. A. M. Aslam, T. R. rashid, and G. M. Murtaza, "Hybrid encryption for image security using improved Henon map with sine and cosine and Arnold's transformation," Sep. 27, 2024. doi: 10.21203/rs.3.rs-4975978/v1.

[29] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018, doi: 10.1016/j.sigpro.2018.06.008.

[30] B. K. ShreyamshaKumar and C. R. Patil, "JPEG image encryption using fuzzy PN sequences," *Signal Image Video Process*, vol. 4, no. 4, pp. 419–427, Nov. 2010, doi: 10.1007/s11760-009-0131-6.