Sistemasi: Jurnal Sistem Informasi
Volume 15, Nomor 5, 2026: 1608-1619
ISSN:2302-8149
e-ISSN:2540-9719

Modifikasi Mode *Cipher Feedback* berbasis *Dynamic Key Hénon Map* untuk Pengamanan Data Citra

Modified Cipher Feedback Mode based on a Dynamic Hénon Map Key for Image Data Security

[1]Naufal Zafrany Syamsudin, [2]Nur Rochmah Dyah Puji Astuti*
[1,2]Program Studi Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan
[1,2]Jl. Ki Ageng Pamenahan, Yogyakarta 55191, Indonesia
*e-mail: rochmahdyah@tif.uad.ac.id

(***received*:** 1 April 2026, ***revised*:** 30 April 2026, ***accepted*:** 9 May 2026)

Abstrak

Keamanan transmisi citra digital rentan terhadap serangan analisis statistik akibat tingginya korelasi spasial antar piksel. Selain itu, penggunaan sistem *chaos* pada perangkat digital juga kerap mengalami masalah degradasi periodik. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan modifikasi mode operasi *Cipher Feedback* (CFB) yang diintegrasikan dengan pembangkit kunci dinamis berbasis *Hénon Map*. Kontribusi utama penelitian ini adalah penggunaan *hash* SHA-256 untuk inisialisasi parameter awal, serta pemanfaatan nilai *ciphertext* sebagai umpan balik (perturbasi) guna memperbarui parameter *Hénon Map* di setiap iterasi. Evaluasi algoritma dilakukan terhadap 25 citra uji dalam format *grayscale* dan RGB. Hasil pengujian mencatat rata-rata nilai Entropi Shannon sebesar 7,998, dengan metrik sensitivitas diferensial NPCR mencapai 99,606% dan UACI 33,464%. Sementara itu, proses dekripsi menghasilkan nilai *Root Mean Square Error* (RMSE) 0 dan *Peak Signal-to-Noise Ratio* (PSNR) 100 dB. Data tersebut mengindikasikan bahwa arsitektur yang diusulkan mampu memitigasi degradasi *chaos*, memiliki resistensi terhadap *chosen-plaintext attacks*, dan dapat merekonstruksi data visual tanpa adanya degradasi informasi (*lossless*).

Kata kunci: enkripsi citra, kunci dinamis, modifikasi CFB, peta hénon, sistem chaos

Abstract

The security of digital image transmission is vulnerable to statistical analysis attacks due to the high spatial correlation among pixels. In addition, the implementation of chaotic systems on digital devices often suffers from periodic degradation problems. To address these issues, this study proposes a modified Cipher Feedback (CFB) mode integrated with a dynamic key generator based on the Hénon Map. The main contribution of this research lies in the use of SHA-256 hashing for initializing the initial parameters, as well as the utilization of ciphertext values as feedback (perturbation) to update the Hénon Map parameters in each iteration. The proposed algorithm was evaluated using 25 test images in both grayscale and RGB formats. The experimental results achieved an average Shannon entropy value of 7.998, with differential sensitivity metrics reaching 99.606% for the Number of Pixels Change Rate (NPCR) and 33.464% for the Unified Average Changing Intensity (UACI). Meanwhile, the decryption process produced a Root Mean Square Error (RMSE) value of 0 and a Peak Signal-to-Noise Ratio (PSNR) of 100 dB. These findings indicate that the proposed architecture is capable of mitigating chaos degradation, resisting chosen-plaintext attacks, and reconstructing visual data without information degradation (lossless).

Keywords: *chaotic system, dynamic key, hénon map, image encryption, modified CFB*

1 Pendahuluan

Pesatnya pertukaran data visual digital pada era modern, seperti transmisi citra medis, dokumen rahasia, dan komunikasi multimedia, menempatkan keamanan informasi pada tingkat urgensi yang sangat tinggi [1]. Berbeda dengan data teks konvensional, citra digital memiliki karakteristik unik berupa kapasitas penyimpanan yang besar, redundansi data yang tinggi, serta korelasi spasial yang

sangat erat antar piksel yang berdekatan. Jika algoritma enkripsi konvensional diterapkan secara langsung tanpa mode operasi yang tepat seperti penggunaan *Electronic Codebook* (ECB) skema tersebut terbukti gagal menyembunyikan pola visual asli karena setiap blok data yang identik akan menghasilkan blok *ciphertext* yang sama [2]. Kondisi ini menuntut adanya mekanisme difusi tingkat tinggi yang mampu memutus korelasi antar piksel secara drastis, sehingga citra terenkripsi berubah sepenuhnya menjadi *noise* acak yang tidak dapat diidentifikasi secara visual maupun dipecahkan menggunakan analisis statistik [3].

Sebagai alternatif solusi untuk memecahkan kebuntuan pada enkripsi citra, penerapan mode operasi seperti *Cipher Feedback* (CFB) menjadi langkah komputasi yang sangat rasional. Arsitektur CFB memiliki keunggulan fundamental dalam mentransformasikan algoritma berbasis blok menjadi *stream cipher* yang dapat menyinkronkan dirinya sendiri secara dinamis [4]. Kemampuan ini memungkinkan data citra dieksekusi dalam unit yang jauh lebih kecil (seperti pemrosesan 8-bit per piksel) tanpa memerlukan proses penambahan bit semu (*padding*) yang membebani komputasi. Lebih jauh lagi, mekanisme CFB secara efektif mematahkan repetisi pola visual melalui skema umpan balik antar *ciphertext*, yang memastikan tingkat pengacakan yang tinggi pada data citra [4], [5]. Namun, meskipun mekanisme perantaian data CFB diakui sangat tangguh, kekuatan enkripsi tersebut pada akhirnya berpusat secara absolut pada tingkat keacakan, ketidakteraturan, dan kompleksitas dari aliran kunci (*keystream*) yang diaplikasikan.

Dalam ranah kriptografi modern, sistem dinamik *chaos* khususnya peta dua dimensi yang kompleks seperti Hénon Map telah diakui sebagai kandidat ideal untuk pembangkitan kunci *pseudo-random*. Hal ini didasari oleh sifat ergodik dan sensitivitasnya yang ekstrem terhadap kondisi awal, yang lebih dikenal dengan istilah *butterfly effect* [6], [7]. Kendati demikian, pernyataan masalah (*problem statement*) utama dalam riset ini bermuara pada implementasi matematis sistem *chaos* ke dalam perangkat keras atau lunak digital. Komputer modern beroperasi dengan batasan presisi komputasi yang terbatas (*finite computing precision*), yang secara inheren memicu terjadinya fenomena degradasi dinamis (*dynamical degradation*) pada sistem *chaos* [8]. Keterbatasan digital ini menyebabkan lintasan *chaos* yang seharusnya acak dan tak berujung pada akhirnya akan tereduksi dan jatuh ke dalam orbit periodik yang sangat pendek (*short periodic windows*). Akibatnya, kunci kriptografi yang dihasilkan akan mengalami siklus pengulangan, sehingga sistem menjadi sangat rentan diretas melalui serangan analisis frekuensi maupun eksploitasi ruang fase oleh para kriptanalis [8], [9].

Untuk mengatasi celah keamanan tersebut, penelitian ini bertujuan untuk merancang dan mengevaluasi skema enkripsi citra hibrida yang mengintegrasikan sistem *chaos* Hénon Map sebagai pembangkit kunci dinamis ke dalam arsitektur modifikasi mode *Cipher Feedback* (CFB). Signifikansi dan manfaat utama dari kegiatan penelitian ini adalah menghasilkan sistem kriptografi visual mutakhir yang: (1) memiliki ruang pencarian kunci yang sangat masif dan tahan terhadap serangan *brute-force* karena proses inisialisasi awal sepenuhnya dikendalikan oleh *hashing* SHA-256; (2) mampu mencegah terjadinya fenomena degradasi dinamis pada *chaos* digital melalui pemanfaatan nilai umpan balik *ciphertext* dari modul CFB sebagai mekanisme perturbasi parameter; serta (3) menciptakan arsitektur keamanan data citra yang bersifat *lossless* dan sangat tangguh dalam menahan serangan *differential cryptanalysis* tanpa membebani kecepatan komputasi sistem.

Meskipun penggunaan sistem *chaos* dan mode operasi CFB telah banyak diteliti, terdapat celah penelitian (*research gap*) yang signifikan dalam literatur saat ini. Sebagian besar skema enkripsi berbasis *chaos* digital masih terjebak dalam dilema antara keamanan dan efisiensi. Metode yang sangat aman seperti *Genetic Algorithm* (GA) [10] atau *Coupling Chaotic Map* ganda [4] membutuhkan beban komputasi yang sangat tinggi, sehingga tidak ideal untuk aplikasi *real-time*. Di sisi lain, sistem *chaos* yang lebih ringan sering kali rentan terhadap fenomena degradasi periodik [8] dan serangan *chosen-plaintext attacks* (CPA) karena penggunaan parameter yang statis [9]. Belum ditemukan solusi yang secara spesifik mampu mengatasi degradasi periodik pada *Hénon Map* digital secara efisien tanpa mengorbankan kecepatan operasional *stream cipher*.

2 Tinjauan Literatur

Dalam dunia keamanan transmisi data visual digital, dibutuhkan algoritma kriptografi yang tidak hanya ringan secara komputasi, tetapi juga benar-benar tahan terhadap berbagai bentuk analisis

 ISSN:2302-8149
e-ISSN:2540-9719

statistik maupun ruang fase. Beberapa studi belakangan ini mulai melirik sistem chaos sebagai basis pembangkit kunci dalam enkripsi citra. Hameed dkk. [7] menunjukkan bahwa sistem berbasis chaos unggul dalam menyembunyikan redundansi data visual, berkat karakteristik ergodiknya yang khas. Sayangnya, sebagian besar skema enkripsi yang ada masih bertumpu pada sistem chaos satu dimensi seperti Logistic Map yang memiliki kelemahan mendasar: ruang parameter kuncinya terlalu sempit dan deret kuncinya rentan diprediksi lewat rekonstruksi ruang fase [9]. Kondisi ini mendorong peneliti beralih ke sistem chaos berdimensi lebih tinggi. Kanwal dkk. [11] dan Zhang dkk. [12] mengkaji peta chaos dua dimensi seperti Hénon Map, dan keduanya sepakat bahwa sistem 2D jauh lebih mampu menangani korelasi spasial antar piksel yang erat, terutama pada algoritma enkripsi citra berwarna.

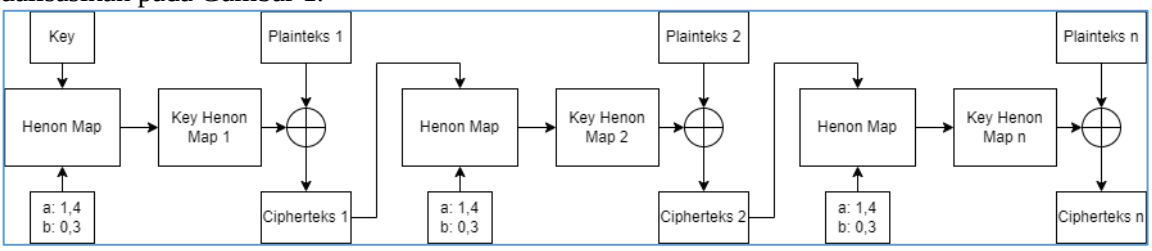
Namun, Hénon Map pun tidak luput dari tantangan teknis saat diimplementasikan secara digital. El-Den dkk. [8] mengingatkan bahwa keterbatasan presisi floating-point pada perangkat keras modern berpotensi memicu degradasi dinamis pada sistem chaos lintasan chaos bisa terperangkap dalam siklus periodik pendek yang berujung pada pengulangan kunci. Untuk mengatasi hal ini, sejumlah peneliti menawarkan solusi seperti Genetic Algorithm (GA) untuk pembentukan kunci dinamis [10] atau arsitektur Coupling Chaotic Map ganda [4]. Namun kedua pendekatan tersebut berbayar mahal: waktu komputasi membengkak drastis, sehingga kurang cocok untuk keperluan enkripsi citra secara langsung (real-time).

Masalah lain yang tak kalah penting adalah pemilihan mode operasi enkripsi itu sendiri. Xia dkk. [2] dan Gafur dkk. [13] mengulas kelemahan mode ECB dan CBC, di mana pola visual pada citra asli masih bisa terbaca samar di ciphertext. Mode CFB kemudian muncul sebagai alternatif yang lebih baik karena mampu mengubah block cipher menjadi stream cipher [14], [4]. Namun arsitektur CFB konvensional punya masalah tersendiri: keystream dibangkitkan secara bertahap dengan mengenkripsi ciphertext sebelumnya menggunakan algoritma berat seperti AES, yang terlalu lambat untuk citra beresolusi tinggi [15]. Di sisi lain, Zhu dkk. [16] memperingatkan bahwa XOR langsung terhadap aliran bit chaos tanpa mekanisme umpan balik rentan terhadap differential cryptanalysis karena tidak adanya efek longsoran antar blok.

Dari berbagai penelitian di atas, terlihat jelas satu celah yang belum terisi: belum ada skema yang berhasil menggabungkan kecepatan XOR stream cipher, kompleksitas Hénon Map, dan ketahanan umpan balik CFB, sekaligus menyelesaikan masalah degradasi periodik tanpa mengorbankan efisiensi. Atas dasar itulah, artikel ini hadir dengan rancangan "Arsitektur Modifikasi CFB Berbasis Chaos". Berbeda dari CFB konvensional yang mengandalkan algoritma enkripsi statis, pendekatan yang diusulkan di sini bekerja dengan cara menyuntikkan nilai ciphertext saat ini (C_i) langsung sebagai umpan balik untuk mengganggu parameter internal (x, y) Hénon Map pada iterasi berikutnya. Dengan dikombinasikan pada inisialisasi awal berbasis hash SHA-256, sistem ini diyakini mampu mengatasi degradasi chaos secara lebih elegan, menjaga entropi citra pada level ideal, dan menekan korelasi antar piksel hingga mendekati nol dengan beban komputasi yang jauh lebih ringan dibanding metode evolusioner yang ada.

3 Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental algoritmik untuk merancang, mengimplementasikan, dan mengevaluasi performa keamanan dari sebuah arsitektur kriptografi citra. Eksperimen komputasi dikembangkan menggunakan bahasa pemrograman Python 3 pada lingkungan perangkat keras berspesifikasi prosesor Intel Core i7 dengan RAM 16 GB. Fokus utama metode ini adalah perancangan arsitektur modifikasi mode *Cipher Feedback* (CFB) yang dinamis menggunakan generator *chaos* Hénon Map. Aliran data dari tahapan inisialisasi kunci hingga ekstraksi *ciphertext* divisualisasikan pada Gambar 1.



 ISSN:2302-8149
e-ISSN:2540-9719

Gambar 1 Diagram alur algoritma

Berdasarkan arsitektur pada Gambar 1, algoritma enkripsi dibangun melalui pendekatan modular yang terdiri dari empat tahapan perhitungan matematis dan satu tahapan evaluasi teknis:

3.1 Inisialisasi Parameter Berbasis SHA-256

Mayoritas sistem *chaos* memiliki kelemahan mendasar pada penggunaan parameter awal yang statis. Algoritma ini memetakan *password* pengguna menjadi nilai awal menggunakan fungsi *hash* SHA-256 [17]. Keluaran *hash* dipecah menjadi dua *integer* 64-bit tak bertanda (H_1 dan H_2). Nilai H_1dan H_2dibagi dengan batas maksimum integer 64-bit ($2^{64}-1$) untuk menormalisasinya menjadi nilai pecahan desimal di rentang 0 hingga 1. Nilai pecahan ini kemudian dikalikan dengan lebar domain dan digeser sesuai batas bawahnya, agar hasil pemetaan tepat jatuh ke dalam wilayah *strange attractor* dari Hénon Map, yakni $X \in [-1.5,1.5]$dengan lebar domain 3,0 dan $Y \in [-0.45,0.45]$dengan lebar domain 0,9. Pemilihan batas rentang domain ini mengacu pada pemodelan ruang fase (*phase space*) sistem dinamik yang direferensikan oleh modul komputasi *University of Colorado* [18]. Rentang ini terbukti paling optimal untuk menangkap seluruh lintasan fraktal *strange attractor* tanpa mengalami divergensi komputasi. Perhitungan pemetaannya dirumuskan seperti pada Persamaan (1):

$$X_0 = \left(\frac{H_1}{2^{64}} \times 3.0\right) - 1.5$$

$$Y_0 = \left(\frac{H_2}{2^{64}} \times 0.9\right) - 0.45 \quad (1)$$

Implementasi komputasional dari pemetaan matematis tersebut secara berurutan dijabarkan melalui instruksi *pseudo-code* pada Algoritma 1.

Algoritma 1
Pseudocode of Get_Initial_Value

```
Pw : Password (String)
x0, y0 : Initial_Values (Float)
X_min = -1.5, X_width = 3.0
Y_min = -0.45, Y_width = 0.9
Max_64 = 18446744073709551615
Hash_Digest ← Generate SHA-256 hash from Pw
H1 ← Convert bytes 0 to 7 of Hash_Digest to 64-bit Integer
H2 ← Convert bytes 8 to 15 of Hash_Digest to 64-bit Integer
x_norm ← H1 / Max_64
y_norm ← H2 / Max_64
x0 ← (x_norm * X_width) + X_min
y0 ← (y_norm * Y_width) + Y_min
Return x0, y0
```

3.2 Ekstraksi Keystream Presisi Ganda

Komputer modern merepresentasikan nilai variabel *chaos* (x, y) dalam format *floating-point* presisi ganda 64-bit sesuai standar IEEE 754 [8]. Pada format IEEE 754, bit penanda (*sign*) dan eksponen di bagian awal sangat jarang berubah. Sebaliknya, bit *mantissa* di bagian tengah hingga akhir justru sangat sensitif terhadap galat komputasi berantai dan efek longsoran (*avalanche effect*). Atas dasar itulah, fungsi ini secara spesifik mengekstrak memori pada *byte* ke-4 hingga ke-7 yang memiliki fluktuasi tertinggi. Secara spesifik, ekstraksi area *mantissa* pada *byte* tersebut dipilih karena merupakan parameter paling rentan terhadap perubahan mikroskopis. Hal ini menjadi kunci penting untuk secara instan memicu efek longsoran (*avalanche effect*) pada aliran *keystream* yang dibangkitkan. Untuk mereduksi 4 *byte* tersebut menjadi 1 *byte* kunci (*keystream*) 8-bit tanpa kehilangan entropinya, diterapkan operasi logika *Exclusive-OR* ($\oplus$) bertingkat, dengan rumusan matematis pada Persamaan (2):

 ISSN:2302-8149
e-ISSN:2540-9719

$$k_{xi} = x_{i(4)} \oplus x_{i(5)} \oplus x_{i(6)} \oplus x_{i(7)}$$
$$k_{yi} = y_{i(4)} \oplus y_{i(5)} \oplus y_{i(6)} \oplus y_{i(7)}$$
$$k_i = k_{xi} \oplus {}_{yi} \quad (2)$$

Langkah-langkah ekstraksi bit memori dan operasi logika reduksi ini diwujudkan ke dalam blok fungsi pada Algoritma 2.

Algoritma 2
Pseudocode of Convert_To_Key_Byte

```
x, y : Chaos_Variables (Float)
K_byte : Keystream_Byte (Integer)
x_bits ← Convert x to 64-bit IEEE 754 byte array
y_bits ← Convert y to 64-bit IEEE 754 byte array
x_key ← x_bits[4] XOR x_bits[5] XOR x_bits[6] XOR x_bits[7]
y_key ← y_bits[4] XOR y_bits[5] XOR y_bits[6] XOR y_bits[7]
K_byte ← x_key XOR y_key
Return K_byte
```

3.3 Perturbasi Status Modifikasi CFB

Modifikasi CFB dilakukan pada fase umpan balik untuk memecahkan masalah degradasi periodik digital [4]. Pada tahap ini, *ciphertext* (C_i) digunakan untuk melakukan perturbasi terhadap koordinat sistem *chaos*. Nilai $C_i$dibagi dengan 255.0 lalu dikurangi 0.5, sehingga blok *ciphertext* terkonversi menjadi gangguan mikroskopis (C_{norm}) dengan rentang $[-0.5, 0.5]$ yang berimbang. Ketika gangguan ini ditambahkan ke nilai $x$dan y, ada risiko koordinat terlempar keluar dari batas *strange attractor*. Untuk mencegah divergensi tersebut, diterapkan operasi aritmatika modular (MOD) terhadap lebar domain, yakni 3.0 untuk X dan 0.9 untuk Y. Operasi ini bekerja sebagai mekanisme pelipatan (*folding mechanism*). Modifikasi arsitektur ini memberikan nilai keunggulan utama: sistem tidak memerlukan proses iterasi evolusioner yang berat secara komputasi, namun secara efektif mampu memutus fenomena degradasi periodik digital secara dinamis dengan menjaga lintasan *chaos* tetap terkunci di dalam batas aman *strange attractor*, seperti ditunjukkan pada Persamaan (3):

$$x'_{i+1} = \left((x_{i+1} + c_{norm} + 1.5)\ mod\ 3.0\right) - 1.5$$
$$y'_{i+1} = \left((y_{i+1} + c_{norm} + 0.45)\ mod\ 0.9\right) - 0.45 \quad (3)$$

Mekanisme injeksi gangguan dinamis dan pelipatan modular tersebut secara algoritmik direpresentasikan pada Algoritma 3.

Algoritma 3
Pseudocode of Perturb_State

```
x, y : Current_Chaos_Variables (Float)
C_byte : Ciphertext_Byte (Integer)
x_new, y_new : Perturbed_Variables (Float)
X_min = -1.5, X_width = 3.0
Y_min = -0.45, Y_width = 0.9
C_norm ← (C_byte / 255.0) - 0.5
x_new ← ((x + C_norm - X_min) MOD X_width) + X_min
y_new ← ((y + C_norm - Y_min) MOD Y_width) + Y_min
Return x_new, y_new
```

3.4 Orkestrasi Enkripsi Utama

Fungsi ini mensinkronisasi seluruh proses secara sekuensial. Iterasi diawali dengan fase pemanasan (*warm-up*) sebanyak 200 kali. Tahap ini tidak menghasilkan keluaran apapun, tetapi perannya cukup krusial: membuang efek transien sekaligus memutus korelasi linier antara *password* awal dengan deret keluaran yang akan dibangkitkan. Setelah itu, sistem mengiterasi persamaan diskrit Hénon Map menggunakan parameter klasik $a = 1.4$ dan $b = 0.3$yang pertama kali dibuktikan oleh

 ISSN:2302-8149
e-ISSN:2540-9719

Hénon [6]. Pemilihan nilai konstanta klasik ini menjadi standar justifikasi bahwa sistem dijamin beroperasi di dalam rezim *strange attractor* dengan sifat ergodik yang stabil. Lebih lanjut, penggunaan 200 iterasi *warm-up* divalidasi sebagai langkah krusial untuk membuang efek transien dan memutus total korelasi linear antara *password* asli dengan deret kunci. Untuk memastikan sistem beroperasi dalam rezim *strange attractor*, digunakan pemetaan diskrit yang dinyatakan pada Persamaan (4)

$$x_{i+1} = 1 - 1.4x_i^2 + y_i$$
$$y_{i+1} = 0.3x_i \quad (4)$$

Setiap blok *keystream* yang dibangkitkan kemudian di-XOR-kan dengan *plaintext* ($C_i = P_i \oplus K_i$). Nilai *ciphertext* yang dihasilkan lalu diinjeksikan kembali ke dalam sistem, sehingga lintasan *chaos* terdistorsi secara langsung. Inilah yang menciptakan efek perantaian data (*data chaining*), di mana satu perubahan pada satu piksel saja akan merambat secara eksponensial ke seluruh blok citra. Integrasi dari seluruh fase mulai dari pemanasan hingga enkripsi berantai dieksekusi melalui orkestrasi fungsi utama sebagaimana dijabarkan pada Algoritma 4.

Algoritma 4
Pseudocode of Process_Encryption

```
P_array : Plaintext_Bytes_Array
C_array : Ciphertext_Bytes_Array
x0, y0 : Initial_Chaos_Values (Float)
a = 1.4, b = 0.3
Initialize C_array as empty list []
x ← x0
y ← y0
For i from 1 to 200 do:
    x_next ← 1 - a * x^2 + y
    y_next ← b * x
    dummy_key ← Execute Algoritma 2 with (x_next, y_next)
    x, y ← Execute Algoritma 3 with (x_next, y_next, dummy_key)
End For
For each P_byte in P_array do:
    x_map ← 1 - a * x^2 + y
    y_map ← b * x
    K_byte ← Execute Algoritma 2 with (x_map, y_map)
    C_byte ← P_byte XOR K_byte
    Add C_byte to C_array
    x , y ← Execute Algoritma 3 with (x_map, y_map, C_byte)
End For
Return C_array
```

3.5 Evaluasi Keamanan dan Integritas Data

Untuk mengukur efektivitas dan ketahanan algoritma yang diusulkan, evaluasi dilakukan menggunakan deretan metrik kriptografi standar. Penilaian didasarkan pada definisi operasional dan perhitungan matematis berikut:

3.5.1 Entropi Shannon

Digunakan untuk mengkuantifikasi derajat ketidakpastian informasi dalam memori [19]. Sistem yang kuat akan mendistribusikan probabilitas kemunculan nilai byte (0-255) secara merata dengan target entropi teoretis mendekati 8,0 bit/byte, dihitung menggunakan Persamaan (5):

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \quad (5)$$

 ISSN:2302-8149
e-ISSN:2540-9719

3.5.2 Sensitivitas Diferensial (NPCR dan UACI)

Ketahanan terhadap serangan kriptanalisis diferensial divalidasi dengan sengaja memodifikasi satu nilai piksel pada citra sumber [20]. Dampak rambatan modifikasi tersebut ke seluruh *ciphertext* diukur melalui persentase piksel yang berubah (NPCR) dan rata-rata intensitas perubahan warnanya (UACI). Sebagai pembanding validasi standar teoretis, nilai ekspektasi yang menjadi rujukan ideal adalah 99,609% untuk NPCR dan 33,463% untuk UACI, sebagaimana dirumuskan pada Persamaan (6):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (6)$$

3.5.3 Integritas Pemulihan (PSNR dan RMSE)

Mengingat sistem dapat diaplikasikan untuk data visual sensitif, perhitungan *Mean Square Error* (MSE) dan *Root Mean Square Error* (RMSE) digunakan untuk mengonfirmasi ketiadaan galat pada citra hasil dekripsi [21]. Nilai RMSE = 0 dan nilai tak terhingga pada PSNR (secara komputasi direpresentasikan sebagai 100 dB) menjadi bukti absolut bahwa algoritma bersifat *lossless* (pulih sempurna), dengan perhitungan yang merujuk pada Persamaan (7):

$$MSE = \frac{1}{W \times H} \sum_{i,j} (P(i,j) - P'(i,j))^2$$

$$PSNR = 10 \log 10 \left(\frac{255^2}{MSE}\right)$$

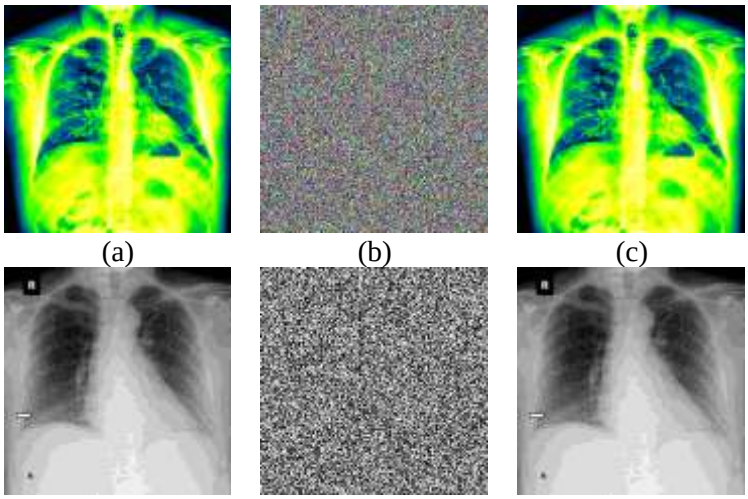
$$RMSE = \sqrt{MSE} \quad (7)$$

4 Hasil dan Pembahasan

Implementasi dan pengujian algoritma modifikasi *Cipher Feedback* (CFB) berbasis *Hénon Map* dikerjakan menggunakan bahasa pemrograman *Python* 3. Pengujian dilakukan pada 25 citra uji yang bersumber dari dataset *Kaggle*, terdiri dari 15 citra *RGB* dan 10 citra *grayscale*, seluruhnya telah diseragamkan ke resolusi 256×256 piksel. Hasil pengujian kemudian dievaluasi secara kuantitatif maupun kualitatif guna mengukur sejauh mana sistem mampu bertahan dalam beberapa skenario pengujian standar kriptografi.

4.1 Hasil Visualisasi Enkripsi dan Dekripsi

Pengujian kualitatif pertama dilakukan dengan mengamati perubahan pola visual citra. Citra asli (*plaintext*) dienkripsi menggunakan parameter inisialisasi yang dibangkitkan dari fungsi *hash* SHA-256. Hasil enkripsi visual ditunjukkan pada Gambar 2.



(a) (b) (c)

 ISSN:2302-8149
e-ISSN:2540-9719

(d) (e) (f)

Gambar 2 Hasil visualisasi pengujian: (a) *Plaintext* Citra 1, (b) *ciphertext* citra 1, (c) hasil dekripsi citra 1, (d) *plaintext* citra 2, (e) *ciphertext* citra 2, (f) hasil dekripsi citra 2

Berdasarkan visualisasi pada Gambar 2(b), citra *ciphertext* yang dihasilkan tampak menyerupai derau acak (*random noise*), di mana kontur maupun tekstur dari citra asli sudah tidak dapat dikenali secara visual sama sekali. Menurut Zolfaghari dan Koshiba [22], tersamarkannya fitur spasial pada *ciphertext* ini merupakan indikator bahwa algoritma mampu menjalankan fungsi pengacakan (*confusion*) dengan cukup efektif.. Sementara itu, Gambar 2(c) memperlihatkan bahwa citra berhasil direkonstruksi kembali secara utuh menggunakan kunci yang benar.

4.2 Analisis Entropi Shannon

Entropi Shannon digunakan untuk mengukur seberapa acak distribusi nilai intensitas piksel pada suatu citra. Pada citra digital 8-bit, nilai entropi maksimal secara teoretis adalah 8,0 bit/byte. Hasil pengukuran entropi rata-rata dari keseluruhan dataset ditampilkan pada Tabel 1.

Tabel 1 Hasil analisis entropy

Nama	Format	Entropy
gambar1.png	RGB	7,999
gambar2.png	RGB	7,999
gambar3.png	RGB	7,999
gambar4.png	RGB	7,999
gambar5.png	RGB	7,999
gambar6.png	RGB	7,999
gambar7.png	RGB	7,999
gambar8.png	RGB	7,999
gambar9.png	RGB	7,999
gambar10.png	RGB	7,999
gambar11.png	RGB	7,999
gambar12.png	RGB	7,999
gambar13.png	RGB	7,999
gambar14.png	RGB	7,999
gambar15.png	RGB	7,999
gambar16.png	Grayscale	7,997
gambar17.png	Grayscale	7,998
gambar18.png	Grayscale	7,997
gambar19.png	Grayscale	7,997
gambar20.png	Grayscale	7,997
gambar21.png	Grayscale	7,997
gambar22.png	Grayscale	7,997
gambar23.png	Grayscale	7,998
gambar24.png	Grayscale	7,997
gambar25.png	Grayscale	7,997

Tabel 1 memperlihatkan bahwa rata-rata nilai entropi pada citra *ciphertext* mencapai 7,998, angka yang sangat dekat dengan batas teoretis maksimalnya yakni 8,0. Hal ini mengindikasikan bahwa sistem telah bekerja dengan baik dalam menyebarkan frekuensi kemunculan nilai warna piksel secara merata ke seluruh rentang 0 hingga 255. Capaian dari arsitektur modifikasi CFB yang diusulkan ini sejalan dengan performa skema enkripsi terkini di literatur, seperti algoritma *multi-chaotic* dan pengkodean DNA yang dikembangkan oleh Wang dkk. [23] yang juga sukses mencatat nilai entropi mendekati batas ideal 8,0. Secara matematis, nilai 7,998 menunjukkan bahwa citra *ciphertext* memiliki tingkat keacakan yang memadai, sehingga upaya *kriptanalisis* berbasis statistik (*statistical attacks*) menjadi jauh lebih sulit dilakukan. Secara praktikal, pencapaian entropi rata-rata sebesar 7,998 ini mengindikasikan bahwa algoritma mampu secara signifikan mendegradasi korelasi spasial yang erat pada citra asli. Distribusi frekuensi piksel yang mendekati seragam membuat citra

 ISSN:2302-8149
e-ISSN:2540-9719

ciphertext kehilangan rekam jejak visual aslinya, sehingga menyulitkan upaya pengenalan pola yang umumnya digunakan oleh kriptanalis untuk mengekstrak informasi.

4.3 Analisis Sensitivitas Diferensial (NPCR dan UACI)

Pengujian ini bertujuan untuk melihat seberapa sensitif algoritma terhadap perubahan kecil pada citra asli, atau yang lebih dikenal sebagai resistensi terhadap *differential cryptanalysis*. Caranya cukup sederhana: citra asli dienkripsi terlebih dahulu menghasilkan C_1, lalu satu piksel dipilih secara acak dan nilainya diubah, kemudian citra yang telah dimodifikasi tersebut dienkripsi kembali menghasilkan C_2.

Tabel 2 Hasil analisis sensitivitas diferensial

Nama	Format	NPCR	UACI
gambar1.png	RGB	99,595	33,539
gambar2.png	RGB	99,613	33,485
gambar3.png	RGB	99,610	33,400
gambar4.png	RGB	99,606	33,578
gambar5.png	RGB	99,585	33,374
gambar6.png	RGB	99,616	33,486
gambar7.png	RGB	99,597	33,504
gambar8.png	RGB	99,605	33,465
gambar9.png	RGB	99,603	33,506
gambar10.png	RGB	99,639	33,589
gambar11.png	RGB	99,604	33,475
gambar12.png	RGB	99,600	33,550
gambar13.png	RGB	99,586	33,391
gambar14.png	RGB	99,593	33,476
gambar15.png	RGB	99,585	33,374
gambar16.png	Grayscale	99,610	33,440
gambar17.png	Grayscale	99,623	33,401
gambar18.png	Grayscale	99,604	33,356
gambar19.png	Grayscale	99,606	33,528
gambar20.png	Grayscale	99,635	33,425
gambar21.png	Grayscale	99,596	33,499
gambar22.png	Grayscale	99,634	33,459
gambar23.png	Grayscale	99,615	33,449
gambar24.png	Grayscale	99,590	33,516
gambar25.png	Grayscale	99,610	33,333

Berdasarkan Tabel 2, algoritma yang diusulkan menghasilkan rata-rata NPCR sebesar 99,606% dan UACI sebesar 33,464%. Angka ini sangat mendekati nilai ekspektasi teoretis standar, yakni NPCR $\approx 99.6094\%$ dan UACI $\approx 33.4635\%$ [20]. Performa tersebut tidak lepas dari peran mekanisme injeksi pada modifikasi CFB (Algoritma 3), di mana nilai *ciphertext* disuntikkan kembali sebagai variabel perturbasi yang memicu *dynamic avalanche effect* secara berkelanjutan. Hasilnya, perubahan sekecil satu piksel pada citra awal terbukti cukup untuk menghasilkan *ciphertext* yang berbeda secara signifikan. Temuan ini menunjukkan bahwa sistem memiliki ketahanan yang baik terhadap upaya manipulasi data maupun *chosen-plaintext attacks* (CPA), menutupi celah kerentanan yang umumnya ditemukan pada arsitektur *chaos* 1D tanpa umpan balik yang dianalisis oleh Fan dkk. [9] melalui pengujian *chosen-plaintext attack*. Analisis mutakhir oleh Wu dan Wang [17] juga menegaskan bahwa arsitektur umpan balik (*feedback*) yang dikombinasikan dengan fungsi *hash* (SHA-256) terbukti mampu meningkatkan ketahanan sistem terhadap serangan diferensial secara signifikan. Pencapaian metrik yang mendekati nilai ekspektasi teoretis ini merupakan indikator efektivitas dari mekanisme injeksi *ciphertext* pada modifikasi CFB yang berhasil memicu *dynamic*

 ISSN:2302-8149
e-ISSN:2540-9719

avalanche effect. Dari perspektif keamanan, mekanisme ini memberikan tingkat resistensi yang tinggi terhadap manipulasi data, karena sistem secara proaktif menggeser lintasan *strange attractor* sehingga meminimalkan celah eksploitasi pada perangkat digital berpresisi terbatas.

4.4 Analisis Integritas Pemulihan Data (PSNR dan RMSE)

Dalam skenario transmisi citra digital, khususnya untuk data yang bersifat sensitif, citra hasil dekripsi seharusnya tidak mengalami penurunan kualitas sama sekali dibandingkan citra aslinya (*lossless*). Untuk memverifikasi hal ini, integritas pemulihan data diukur secara kuantitatif menggunakan tiga metrik, yaitu *Mean Square Error* (MSE), *Root Mean Square Error* (RMSE), dan *Peak Signal-to-Noise Ratio* (PSNR). Seluruh hasil perhitungan untuk dataset citra uji dirangkum pada Tabel 3.

Tabel 3 Hasil analisis integritas pemulihan data

Nama	Format	PSNR	RMSE
gambar1.png	RGB	100 dB	0
gambar2.png	RGB	100 dB	0
gambar3.png	RGB	100 dB	0
gambar4.png	RGB	100 dB	0
gambar5.png	RGB	100 dB	0
gambar6.png	RGB	100 dB	0
gambar7.png	RGB	100 dB	0
gambar8.png	RGB	100 dB	0
gambar9.png	RGB	100 dB	0
gambar10.png	RGB	100 dB	0
gambar11.png	RGB	100 dB	0
gambar12.png	RGB	100 dB	0
gambar13.png	RGB	100 dB	0
gambar14.png	RGB	100 dB	0
gambar15.png	RGB	100 dB	0
gambar16.png	Grayscale	100 dB	0
gambar17.png	Grayscale	100 dB	0
gambar18.png	Grayscale	100 dB	0
gambar19.png	Grayscale	100 dB	0
gambar20.png	Grayscale	100 dB	0
gambar21.png	Grayscale	100 dB	0
gambar22.png	Grayscale	100 dB	0
gambar23.png	Grayscale	100 dB	0
gambar24.png	Grayscale	100 dB	0
gambar25.png	Grayscale	100 dB	0

Tabel 3 memperlihatkan bahwa nilai galat (RMSE) secara konsisten berada di angka 0 untuk seluruh dataset uji, yang secara komputasi tercermin dari nilai PSNR sebesar 100 dB. Mengacu pada tinjauan metrik evaluasi kinerja kriptografi mutakhir oleh Zhang dan Liu [21], kombinasi RMSE 0 dan batas maksimal PSNR tersebut mengindikasikan bahwa proses dekripsi mampu memulihkan citra tanpa mengalami kehilangan kualitas informasi (*zero information loss*). Hasil ini sekaligus memvalidasi bahwa mekanisme pelipatan modular (*folding mechanism*) pada proses perturbasi CFB berjalan dengan presisi yang baik. Sistem terbukti mampu mempertahankan sifat reversibilitas aljabar dari operasi logika *XOR*, sehingga citra hasil dekripsi konsisten dengan struktur aslinya tanpa ada degradasi resolusi maupun pergeseran nilai warna. Keberhasilan dalam memulihkan data tanpa galat (RMSE 0) membawa implikasi penting, khususnya jika diaplikasikan pada transmisi data yang peka terhadap perubahan piksel, seperti dataset citra medis X-Ray pada pengujian ini. Fakta bahwa arsitektur ini beroperasi secara *lossless* memvalidasi bahwa mekanisme pelipatan modular (MOD)

 ISSN:2302-8149
e-ISSN:2540-9719

tidak merusak reversibilitas informasi, menjadikannya sangat relevan untuk kebutuhan pengamanan transmisi data visual sensitif yang menuntut akurasi diagnosis tinggi.

5 Kesimpulan

Penelitian ini membuktikan bahwa integrasi fungsi *hash* SHA-256 dan mekanisme umpan balik *ciphertext* pada modifikasi mode *Cipher Feedback* (CFB) secara efektif mampu memecahkan masalah degradasi periodik pada implementasi *Hénon Map* digital. Tanpa perlu mengandalkan beban komputasi berat dari algoritma evolusioner, arsitektur yang diusulkan mampu menghasilkan *dynamic avalanche effect* yang tangguh. Hasil pengujian memvalidasi bahwa sistem memiliki ketahanan optimal terhadap serangan kriptanalisis statistik dan diferensial, sekaligus menjamin proses rekonstruksi citra secara sempurna (*lossless*). Karakteristik ini menjadikannya sangat relevan dan andal untuk diaplikasikan pada transmisi data visual sensitif yang menuntut akurasi mutlak, seperti halnya citra rekam medis. Namun demikian, penelitian ini masih memiliki beberapa keterbatasan. Evaluasi performa algoritma saat ini berfokus pada ketahanan kriptografis (metrik entropi, NPCR, UACI, dan PSNR) menggunakan citra uji statis beresolusi standar (256×256 piksel). Analisis komprehensif mengenai efisiensi kecepatan komputasi (*execution time analysis*) secara kuantitatif, serta evaluasi konsumsi memori ketika sistem dihadapkan pada pemrosesan dataset citra beresolusi sangat tinggi (seperti 4K) atau citra bervolume besar, belum dicakup dalam cakupan studi ini. Sebagai arah penelitian selanjutnya (*future work*), pengembangan skema ini dapat difokuskan pada pengujian kompleksitas waktu dan implementasinya di tingkat perangkat keras (*hardware-level implementation*) seperti *Field-Programmable Gate Array* (FPGA) atau perangkat *Internet of Things* (IoT) bersumber daya terbatas. Selain itu, ekspansi pengujian arsitektur modifikasi CFB ini terhadap transmisi data visual bergerak, seperti enkripsi *video streaming* secara *real-time*, akan menjadi ruang eksplorasi yang sangat menjanjikan untuk membuktikan efisiensi algoritma pada skala industri.

Referensi

[1] R. Al Ghivary, N. Wulandari, N. Srikandi, and A. M. Nazilatul F, "Peran Visualisasi Data untuk menunjang Analisa Data Kependudukan di Indonesia," 2023.

[2] R. Xia, M. Li, and S. Chen, "*Encryption Modes Identification of Block Ciphers based on Machine Learning*," *International Journal of Network Security & Its Applications*, Vol. 14, No. 5, pp. 1–10, Sep. 2022, DOI: 10.5121/ijnsa.2022.14501.

[3] S. Das *et al.*, "*Multilayered Digital Image Encryption Approach to Resist Cryptographic Attacks for Cybersecurity*," *PeerJ Comput. SCI.*, vol. 11, p. e3260, Oct. 2025, DOI: 10.7717/peerj-cs.3260.

[4] H. Liu, A. Kadir, and C. Xu, "*Color Image Encryption with Cipher Feedback and Coupling Chaotic Map*," *International Journal of Bifurcation and Chaos*, Vol. 30, No. 12, p. 2050173, Sep. 2020, DOI: 10.1142/S0218127420501734.

[5] K. Jain, B. Titus, P. Krishnan, S. Sudevan, P. Prabu, and A. S. Alluhaidan, "*A Lightweight Multi-Chaos-based Image Encryption Scheme for IoT Networks*," *IEEE Access*, Vol. 12, pp. 62118–62148, 2024, DOI: 10.1109/ACCESS.2024.3377665.

[6] M. Hénon, "*A Two-Dimensional Mapping with a Strange Attractor*," *Commun. Math. Phys.*, Vol. 50, No. 1, pp. 69–77, Feb. 1976, DOI: 10.1007/BF01608556.

[7] B. A. Hameed and E. K. Gbashi, "*A Review of Chaotic Maps used for Generating Secure Random Keys*," *BIO Web Conf.*, Vol. 97, p. 00070, Apr. 2024, DOI: 10.1051/bioconf/20249700070.

[8] B. M. El-Den, S. Aldosary, H. Khaled, T. M. Hassan, and W. Raslan, "*Leveraging Finite-Precision Errors in Chaotic Systems for Enhanced Image Encryption*," *IEEE Access*, Vol. 12, pp. 176057–176069, 2024, DOI: 10.1109/ACCESS.2024.3462807.

[9] H. Fan, H. Lu, C. Zhang, M. Li, and Y. Liu, "*Cryptanalysis of an Image Encryption Algorithm based on Random Walk and Hyperchaotic Systems*," *Entropy*, Vol. 24, No. 1, p. 40, Dec. 2021, DOI: 10.3390/e24010040.

[10] P. Mukherjee, H. Garg, C. Pradhan, S. Ghosh, S. Chowdhury, and G. Srivastava, "*Best Fit DNA-based Cryptographic Keys: The Genetic Algorithm Approach*," *Sensors*, Vol. 22, No. 19, p. 7332, Sep. 2022, DOI: 10.3390/s22197332.

[11] S. Kanwal *et al.*, "*An Effective Color Image Encryption based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices*," *Sensors*, Vol. 22, No. 12, p. 4359, Jun. 2022, DOI: 10.3390/s22124359.

[12] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "*Construction of a New 2D Hyperchaotic Map with Application in Efficient Pseudo-Random Number Generator Design and Color Image Encryption*," *Mathematics*, Vol. 11, No. 14, p. 3171, Jul. 2023, DOI: 10.3390/math11143171.

[13] S. Gafur and E. Aribowo, "Studi Pendekatan *Quality & Differential Analysis* terhadap Kinerja Algoritma AES-CBC pada Enkripsi Gambar," Vol. 12, No. 5, pp. 1115–1122, 2025.

[14] S. Kumar, H. Singh, I. Gupta, and A. J. Gupta, "*Symmetric Encryption Scheme based on Quasigroup using Chained Mode of Operation*," Aug. 2024.

[15] H. Alabdulrazzaq and M. N. Alenezi, "*Performance Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish*," *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 14, No. 1, Apr. 2022, DOI: 10.17762/ijcnis.v14i1.5262.

[16] H. Zhu, J. Ge, J. He, and L. Zhang, "*A Non-Degenerate Chaotic Bits XOR System with Application in Image Encryption*," *Math. Comput. Simul.*, Vol. 219, pp. 231–250, May 2024, DOI: 10.1016/j.matcom.2023.12.023.

[17] H. Wu and X. Wang, "*A ROI-based Medical Image Encryption Scheme using Improved Lorenz Chaotic System, Hybrid Pixel-Bit Permutation, and SHA-256 Hashing*," *Advances in Differential Equations and Control Processes*, Vol. 32, No. 4, Oct. 2025, DOI: 10.59400/adecp3511.

[18] University of Colorado Boulder, "*Writing Matlab Functions: The Henon Map*," Department of Mechanical Engineering. Accessed: Jan. 30, 2026. [Online]. Available: http://adjoint.colorado.edu/~daven/Tutorials/dynamics/henon_map.html

[19] S. R. Davies, R. Macfarlane, and W. J. Buchanan, "*Comparison of Entropy Calculation Methods for Ransomware Encrypted File Identification*," *Entropy*, Vol. 24, No. 10, p. 1503, Oct. 2022, DOI: 10.3390/e24101503.

[20] B. Ge, G. Qu, Z. Shen, and J. Lin, "*A Counter Mode and Multi-Channel based Chaotic Image Encryption Algorithm for the Internet of Things*," *Front. Phys.*, Vol. 12, Dec. 2024, DOI: 10.3389/fphy.2024.1494056.

[21] B. Zhang and L. Liu, "*Chaos-based Image Encryption: Review, Application, and Challenges*," *Mathematics*, Vol. 11, No. 11, p. 2585, Jun. 2023, DOI: 10.3390/math11112585.

[22] B. Zolfaghari and T. Koshiba, "*Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap*," *Applied System Innovation*, Vol. 5, No. 3, p. 57, Jun. 2022, DOI: 10.3390/asi5030057.

[23] S. Wang, J. Pan, Y. Cui, Z. Chen, and W. Zhan, "*Fast Color Image Encryption Algorithm based on DNA Coding and Multi-Chaotic Systems*," *Mathematics*, Vol. 12, No. 20, p. 3297, Oct. 2024, DOI: 10.3390/math12203297.