Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

Image Cryptography Process Using Arnold's Cat Map And Henon Map Algorithms

Moch Azhar Al Ghifari[*1], Bayu Surarso[2], Aris Sugiharto[3]

[1]Master Program of Information System, Postgraduate School, Universitas Diponegoro, Indonesia
[2]Department of Mathematics, Universitas Diponegoro, Indonesia
[3]Department of Computer Engineering, Universitas Diponegoro, Indonesia

Email: [1]mochazharalghifari@students.undip.ac.id

Received : Sep 29, 2025; Revised : Dec 22, 2025; Accepted : Jan 19, 2026; Published : Jun 15, 2026

Abstract

The security of digital image data is a crucial aspect in various fields, such as communications, medicine, and the military. The inherent characteristics of digital images—namely high pixel correlation and large data size—render conventional encryption methods less optimal. This study aims to evaluate the encryption quality of images using the Arnold's Cat Map (ACM) and Henon Map algorithms, both individually and in combination (ACM-Henon and Henon-ACM). ACM is utilized to rearrange pixel positions to create a confusion effect, while the Henon Map is employed to randomly alter pixel values (diffusion). The implementation is carried out using the Python programming language within the Visual Studio Code development environment. Encryption quality is assessed using parameters such as Avalanche Effect (AE), Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), and correlation coefficient. Experimental results show that the combined chaos-based methods significantly enhance security compared to the individual algorithms, particularly by analyzing the impact of algorithm order on encryption quality. The best performance was achieved by the Henon→ACM combination, producing NPCR ≈ 99.44%, UACI ≈ 19.93%, entropy ≈ 7.9874, and AE ≈ 50.12%, indicating strong randomness and resistance to differential attacks.

This research demonstrates that combining confusion and diffusion mechanisms yields more secure cipher images than using either method alone. The main contribution of this study lies in providing a systematic comparative evaluation of single and combined chaos-based encryption schemes, including order-sensitive analysis across different image characteristics, rather than proposing a new encryption algorithm. However, the encryption performance is influenced by image size, parameter selection, and iteration count, which may limit consistency across different image characteristics. Future work may explore adaptive parameter optimization and improved diffusion mechanisms for higher UACI values.

Keywords: *Arnold's Cat Map, Henon Map, image encryption, chaotic systems, security validation, evaluation of encryption quality.*

1. INTRODUCTION

In today's digital era, securing image data is increasingly critical in fields such as medicine, military communication, and forensic analysis. Digital images possess high pixel correlation and large data sizes, causing conventional encryption techniques to perform poorly when applied to image structures [1]. Recent work also emphasizes that classical encryption algorithms often fail to provide adequate confusion–diffusion processes, especially when facing statistical attacks on digital images [2]. Other studies similarly report that traditional methods lack sufficient resistance against modern cryptanalytic techniques, motivating the use of more advanced encryption models [3].

Chaos-based methods have attracted considerable attention because chaotic systems exhibit inherent nonlinearity, unpredictability, and sensitivity to initial conditions, making them suitable for secure encryption mechanisms [4]. Several works highlight that chaotic maps can generate strong

randomness and complex diffusion properties needed for robust image protection [5]. Reviews of the latest developments further demonstrate that chaotic systems consistently outperform classical models in resisting correlation and differential attacks [6]. Additional studies report that hybrid chaotic–fuzzy mechanisms can further enhance key sensitivity and statistical strength, showing their promise for image encryption applications [7].

Among various chaotic algorithms, Arnold's Cat Map (ACM) is widely used as a confusion technique because it effectively disrupts the spatial relationships and geometric structures in images [8]. Meanwhile, the Henon Map plays a crucial role in diffusion due to its nonlinear dynamics, enabling strong pixel-value modification across the image [9]. Recent work demonstrates that Henon-based diffusion operations can significantly increase the unpredictability of encrypted images [10]. Studies combining ACM and Henon also show that applying permutation before diffusion improves histogram uniformity and reduces pixel correlation [11]. More advanced hybrid methods have been proposed, including the integration of chaotic maps with optimization techniques to refine permutation sequences [12]. Multi-chaotic layered architectures have also been shown to enhance complexity and improve statistical resistance in encrypted images [13]. Furthermore, color image encryption models based on ACM and Henon demonstrate improved performance in maintaining randomness and visual degradation [14].

Despite this progress, several research gaps remain. Although hybrid and multi-chaotic algorithms have been widely explored, few studies directly compare different ordering sequences of the same chaotic maps, such as ACM→Henon and Henon→ACM [15], [16]. Additionally, many works focus on specific image domains—such as medical images, compressed-domain images, or grayscale datasets—leaving uncertainty regarding consistency across diverse formats including JPG, PNG, BMP, WEBP, and TIFF [17], [18]. Other models, such as 3D chaotic encryptors, have been proposed but seldom compared to lighter two-map combinations like ACM and Henon [19]. Several studies also highlight that performance evaluations frequently omit essential metrics such as NPCR, UACI, Avalanche Effect, and correlation analysis across multi-format datasets [20]. Furthermore, compressed image encryption models have introduced new chaotic dimensions, but their applicability to general image formats remains unsettled [17].

While numerous chaos-based image encryption methods have been proposed, the rationale for selecting specific chaotic maps and the impact of their combination order are not always clearly jusTIFFied. Arnold's Cat Map is widely used for pixel permutation to reduce spatial correlation, whereas the Henon Map is commonly adopted for pixel-value diffusion due to its strong sensitivity to initial conditions [21], [22], [23]. However, the effectiveness of using these maps individually versus in combination, as well as the influence of applying diffusion before or after permutation, has not been systematically evaluated [24], [25]. This study addresses this gap by comparing ACM, Henon Map, and their two combination sequences based on visual and statistical encryption performance.

Therefore, this study aims to evaluate the encryption quality of digital images using Arnold's Cat Map and Henon Map, implemented individually and in two combination sequences. By examining performance across multiple image formats and providing comprehensive quantitative evaluation, this research seeks to determine the optimal chaotic configuration for achieving strong statistical security, high diffusion capability, and improved randomness in encrypted image data.

2. METHOD

In conducting this research, five main work procedures are employed, as illustrated in the flow diagram in Figure 1.

Figure 1 illustrates that this research begins by examining the literature methods that will be employed, including cryptography, chaos theory, Arnold's cat map, Hénon Map, Avalanche effect,

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

Unified Average Changing Intensity, Number of Pixel Change Rate, and Correlation Coefficient. The second stage is data collection, where various image formats (JPG, PNG, BMP, WEBP, and TIFFF) are gathered as test inputs. The third stage involves implementing ACM and Hénon Map algorithms in multiple encryption-order scenarios.

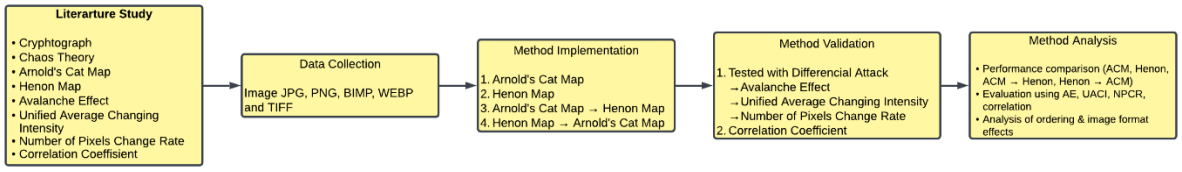


Figure 1. Research Flow Diagram

The fourth stage involves method validation, which is conducted through differential attack testing and the measurement of AE, UACI, NPCR, and correlation values. Finally, the fifth stage is method analysis, which compares algorithm performance and examines the effects of encryption ordering and image formats.

2.1. Literature Study

The first stage involved a literature study to find relevant references from various journals, both local and international. The goal was to understand the methods to be used and how to implement them. The primary focus of this literature study was on cryptographic algorithms, specifically Arnold's Cat Map (ACM) and Hénon, as well as on evaluation methods such as the Avalanche Effect (AE), UACI, NPCR, and the Correlation Coefficient. The study also examined various types of digital images, including PNG, BMP, JPG, TIFF, and WEBP, which are commonly used in image encryption research due to their distinct compression and quality characteristics that impact encryption and decryption results [17].

2.1.1. Cryptography

Since cryptography is a technique for securing plain text messages, such as encrypted key exchange and authentication, while revealing when and where communication is taking place, steganography hides the existence of data to be transmitted [26]. It is then explained that cryptography is a technique based on mathematical calculations to maintain the security, confidentiality, integrity, and authenticity of data [27].

The algorithms used in encryption and decryption require specific keys. The encrypted (or encoded) plaintext message is called ciphertext, while decryption is the process of returning the ciphertext to its original plaintext form. In this study, the cryptographic key is represented by the set of parameters used in both the Arnold's Cat Map and the Henon Map. In chaos-based encryption, these parameters function as the secret key because the encryption and decryption results are highly sensitive to their values .

For the Arnold's Cat Map, the key is the number of iterations applied during the pixel permutation process. For the Henon Map, the key consists of the control parameters (a, b) and the initial conditions (x_0, y_0) that generate the chaotic sequence. The encryption process also depends on the order in which the two chaotic transformations are applied.

Since all these values must be identical during both encryption and decryption, and even a slight variation will produce an incorrect reconstruction, they collectively serve as the cryptographic key in the proposed method. This key representation follows the standard practice in chaos-based image encryption studies.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

2.1.2. Chaos

The term "chaos" describes a highly predictable state of disarray in a complicated natural system. Chaos theory examines systems that appear predictable but behave chaotically [4].

Various methods in this theory include: Logistic Map, ICMIC Map, Tent Map, Chebyshev Map [2], Tinkerbell map, Henon Map, Duffing Map, Arnold Map, Gaus-itated map, etc [5].

2.1.3. Arnold's Cat Map (ACM)

It was first introduced by Vladimir Arnold's in 1960, with the word "cat" used because a picture of a cat was used in his experiments [8]. The Arnold's Cat Map (ACM) transform is a two-dimensional chaos map widely used in obfuscation processes in modern image encryption. One common way to understand its chaotic nature is through its geometric representation on a torus surface, as in the Figure 2.

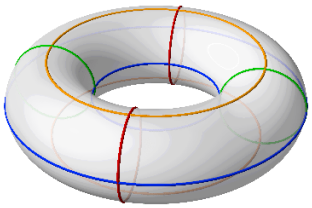


Figure 2. Scheme Continuous Automorphism of the Torus

In this map, pixel coordinates are stretched, rotated, and then folded back together through modulo operations, resulting in complex yet deterministic and reversible positional changes. The visualization of the torus shows how ACM stretches and folds the coordinate plane, a core characteristic of chaotic systems that makes the distribution of pixel positions unpredictable and effective in increasing the degree of image randomness. Recent studies also confirm that linear-modular mappings such as ACM are area-preserving, invertible, and provide significant chaotic mixing effects, making them suitable for the permutation stage of image encryption [28], [29].

Arnold's Cat Map 2D is a pixel randomization algorithm that continuously changes the locations of pixels in an image over many iterations. As the number of iterations increases, the pixel coordinates in the square matrix become repetitive. As the number of iterations increases, the pixel coordinates in the square matrix become repetitive, forming a periodic transformation. In this process, each pixel position (x_i, y_i) is mapped to a new position ($x_i + 1$, $y_i + 1$). The Arnold Cat Map encryption equation can be written as in equation 1 [30].

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod (N) \qquad (1)$$

Where ($x_i + 1$, $y_i + 1$) is the new pixel position after transformation, (x_i , y_i) is the pixel position in the current image, b and c are keys with arbitrary positive integer values, and N is the size of the N x N image. The results of the Arnold Cat Map are reversible, meaning they can be returned to their original form. To restore the encrypted Arnold Cat Map result or the inverse Arnold Cat Map, the following can be written as in equation 2 [30].

$$\begin{bmatrix} x_i \\ y_i \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} \bmod (N) \qquad (2)$$

Various previous studies have shown that using ACM as the initial stage of permutation can increase resistance to statistical attacks and enlarge the key space because the iteration parameters act as cryptographic keys. A study by [31] demonstrated that applying ACM before the diffusion process enhances the randomization of pixel patterns, leading to a more uniform histogram of encrypted images.

Furthermore, studies by [11] and [14] also support that ACM is effective as a confusion mechanism and can provide increased security when combined with other chaotic maps such as Henon, Logistic, or Tent Map. These studies concluded that ACM is not a random generator, but its chaotic structure and periodic nature can improve encryption quality in multi-level systems.

2.1.4. Henon Map

In 1978, the two-dimensional Henon map was proposed by H'enon as a simplified approach to studying the dynamics of Lorenz-Bader systems. [32]. It is a discrete dynamic map that exhibits chaotic behavior, as it is sensitive to its initial conditions [33]. It is defined as in equation 3 and 4.

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (3)$$

$$y_{n+1} = bx_n \quad (4)$$

The behavior of a chaotic system is dependent on the values of parameters a, b that are called control parameters. The parameters and conditions of the Henon map are as follows.

1. **(x_0, y_0)** are the initial conditions of the Henon Map, namely the initial iteration value that determines the starting point of the chaotic system.
2. **a** and **b** are control parameters that govern the behavior of the Henon Map. The values of a and b must be within a certain range to produce stable chaotic behavior.
3. **K = (a, b, x_0, y_0)** is the secret key in the Henon Map-based encryption process, because a small change in one of these values will produce a completely different chaotic output.

The Hénon Map exhibits several strong chaotic properties, including a positive Lyapunov exponent, high sensitivity to initial conditions, pseudo-random behavior, and an approximately uniform distribution across its phase space. These characteristics ensure unpredictability and strong diffusion capability, making the Hénon Map highly suitable for use in cryptographic applications. It is instrumental in determining inherently dynamic sequences, demonstrating the high sensitivity of a condition where the values are initially ordered and exhibit unpredictable attributes in their overall behavior [10].

By expressing changes over time as discrete equations instead of differential equations, Hénon maps are used to examine discrete-time dynamical systems. This characteristic underlies studies of discrete dynamical systems and difference equations [34].

2.1.5. Avalanche Effect (AE)

The Avalanche Effect is a method for determining and understanding the percentage of a message that changes during the encryption process by examining the ratio between the number of bits of the ciphertext that change and the number of bits of the plaintext before it is altered in the encryption process[35].

$$\boldsymbol{AE} = \frac{(\boldsymbol{different\ number\ of\ bits})}{(\boldsymbol{total\ bit})} \times \mathbf{100\%} \quad (5)$$

2.1.6. Unified Average Changing Intensity (UACI)

UACI is designed to try to average the modified intensity between two encrypted images when the difference between the clean (authentic) images is minimal (typically a few pixels) [36]. According to [37], the ideal value for UACI is between 33.25% and 33.48% respectively, and the calculation can be done using the formula [38].

$$\boldsymbol{UACI} = \frac{\mathbf{1}}{\boldsymbol{w} \times \boldsymbol{h}} \sum_{ij} \mathbf{1} \frac{[\boldsymbol{C_1}\,(\boldsymbol{i,j}) - \boldsymbol{C_2}\,(\boldsymbol{i,j})]}{\mathbf{255}} \times \mathbf{100\%} \quad (6)$$

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

Explanation:
W = image width
H = image lenght
C1(i,j) = image result 1 (cipher-image 1)
C2(i,j) = image result 2 (cipher-image 2)

2.1.7. Number of Pixels Change Rate (NPCR)

NPCR and UACI are two percentages used to determine the effect of changing the value of one pixel from the original image to the encrypted image. [39]. According to [37] The ideal value for NPCR is greater than 99.6%, and the calculation can be done using a formula.

$$\boldsymbol{NPCR} = \frac{\sum_{ij} \boldsymbol{D(i,j)}}{\boldsymbol{W \times H}} \times \mathbf{100\%} \quad (7)$$

$$\boldsymbol{D(i,j)} = \begin{cases} \mathbf{0}, \boldsymbol{C_1(i,j)} \neq \boldsymbol{C_2\,(i,j)} \\ \mathbf{1}, \boldsymbol{C_1(i,j)} \neq \boldsymbol{C_2\,(i,j)} \end{cases} \quad (8)$$

Explanation for formula 3:
W = image width
H = image lenght
D (i, j) = the value of the two images being compared (0 or 1)
C1(i, j) = image result1 (cipher-image1)
C2(i, j) = image result2 (cipher-image2)
Explanation for formula 4:
P (m, n) = dimensional original image M x N
P' (m, n) = encrypted image

2.1.8. Correlation Coeffisient

Theoretically, the correlation coefficient between two neighboring pixels ranges from -1 to +1, with a value of ±1 indicating a strong linear relationship and a value close to 0 indicating no correlation at all. In good image encryption, the correlation coefficient value in the cipher-image is expected to approach zero in the horizontal, vertical, and diagonal directions, indicating that the statistical relationship between pixels has been eliminated. This zero value is used as a benchmark for the statistical security of the cipher-image [40].

The similarity between two variables is demonstrated by the correlation method. This coefficient is very useful for calculating the quality of a cryptosystem [39]. This coefficient is particularly useful for computing the cryptosystem's quality, Correlation coefficient is given by [20], [31], [41].

$$F_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (9)$$

Where X and Y are the sets composed of N pixel gray values, $x_i \in X$ and $y_i \in$, are two adjacent pixels,

$$E(X) = \frac{1}{n}\sum_{i=1}^{N} x_i \quad (10)$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N}[X_i - E(X)]^2 \quad (11)$$

$$cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N}[X_i - E(X)]\,[Y_i - E(Y)] \quad (12)$$

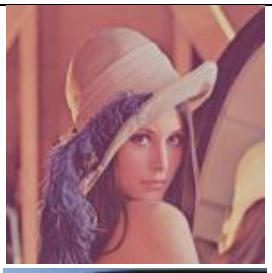
2.2. Data Collection

After conducting literature research, the next step is data collection. In preparing for data collection for this study, image data samples were taken, with the image types being JPG/JPEG, BIMP, TIFFF, WEBP, and BMP. These various formats were selected to test the consistency and effectiveness

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

of the encryption algorithm against varying image file characteristics. The image samples are listed in Table 1 below.

Table 1. Image samples

Name	Image	Image Type	Original Size (dimension)
Lena		JPG	256x256
Sample_png		PNG	426x513
Sample_TIFFf		TIFFF	426x426
Sample1		WEBP	4275x2451
Taz_ref		BMP	400x400

2.3. Method Implementation

The data obtained will then be implemented using a specific method. The methods used in this study are Arnold's Cat Map (ACM) and Hénon Map. This study is divided into three parts: testing the Arnold's Cat Map method separately, testing the Hénon Map method separately, and testing the combined Arnold's Cat Map and Hénon Map methods, as well as their inverses, namely the Hénon Map and Arnold's Cat Map methods. Each method has two processes: encryption and decryption. These two processes are essential parts of cryptography.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

2.3.1. Arnold's Cat Map

For the ACM-only scheme, the resized image is directly encrypted using Arnold's Cat Map with a fixed number of five iterations, which permutes the pixel positions of the image to achieve spatial confusion. The corresponding encryption and decryption processes for the ACM-only scheme are illustrated in Figures 3 and 4.

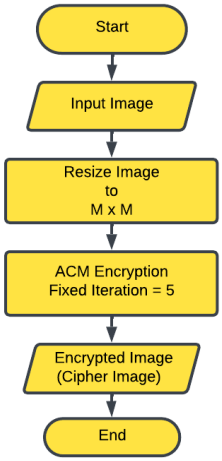


Figure 3. Arnold's Cat Map Encryption Flowchart

Explanation of method encryption flow Arnold's Cat Map from figure 3:

1. Start: Starting point of the method.
2. Input Image: Digital images in RGB or grayscale format are used as system input.
3. Resize Image to M x M: The image is resized to 256 × 256 pixels. This stage aims to: standardize the image size, fulfill the requirements of Arnold's Cat Map which requires the image to be square (square image).
4. ACM Encryption Fixed Iteration = 5: Arnold's Cat Map is applied to permute pixel positions. This process is repeated for 5 fixed iterations, according to the implementation in the source code. This stage aims to eliminate spatial correlation between pixels by randomizing pixel positions.
5. Encrypted Image (Cipher Image) = The result of the permutation process is a cipher image.
6. End: Ending point of the method.

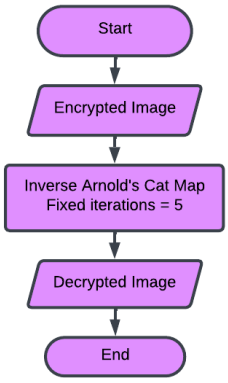


Figure 4. Arnold's Cat Map Decryption Flowchart

Explanation of the method decryption flow metode Henon Map from figure 4:

1. Start: Starting point of the method.
2. Encrypted Image: The result of the permutation process is a cipher image.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

3. Inverse Arnold's Cat Map Fixed Iterations = 5: The permutation is reversed using the inverse ACM with 5 iterations.
4. Decrypted Image: The original image was successfully restored.
5. End: Ending point of the method.

2.3.2. Henon Map

For the Henon-only scheme, the resized image is encrypted using the Henon map as a diffusion mechanism. A chaotic sequence generated by the Henon map is applied to the image through a pixel-wise XOR operation, resulting in pixel value substitution without altering pixel positions. The encryption and decryption processes of the Henon-only scheme are shown in Figures 5 and 6.

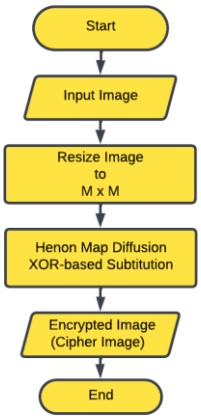


Figure 5. Henon Map Encryption Flowchart

Explanation of method encryption flow Arnold's Cat Map from figure 5:

1. Start: Starting point of the method.
2. Input Image: Digital images in RGB or grayscale format are used as system input.
3. Resize Image to M x M: The image is resized to 256 × 256 pixels. This stage aims to: standardize the image size, fulfill the requirements of Arnold's Cat Map which requires the image to be square (square image).
4. Henon Map Diffusion XOR-based Subtitution: The Henon Map generates a chaotic sequence based on the following parameters: a = 1.4, b = 0.3, and initial conditions $x_0 = 0.1$ and $y_0 = 0.1$. This chaotic sequence is then applied to the pixel values using the XOR operation. This process does not change the pixel positions, but only randomizes the pixel intensity values (pixel substitution).
5. Encrypted Image (Cipher Image): The result of the permutation process is a cipher image.
6. End: Ending point of the method.

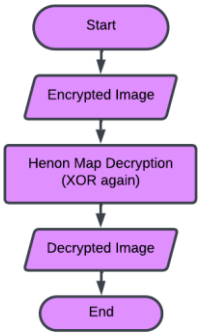


Figure 6. Henon Map Decryption Flowchart

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

Explanation of the method decryption flow metode Henon Map from figure 6:

1. Start: Starting point of the method.
2. Encrypted Image: The result of the permutation process is a cipher image.
3. Henon Map Decyption (XOR again): The XOR operation is reapplied using the same chaotic sequence.
4. Decrypted Image: The original image was successfully restored.
5. End: Ending point of the method

2.3.3. Arnold's Cat Map and Henon Map

In the ACM and Henon scheme, the resized image is first processed using Arnold's Cat Map with five iterations to permute pixel positions. Subsequently, the Henon map is applied as a diffusion stage using an XOR-based substitution of pixel values. This scheme combines confusion followed by diffusion. The corresponding encryption and decryption processes are presented in Figures 7 and 8.

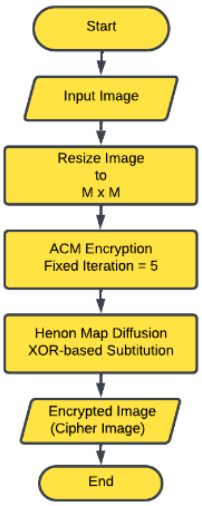


Figure 7. Arnold's Cat Map and Henon Map Enrcryption Flowchart

Explanation of method encryption flow Arnold's Cat Map from figure 7:

1. Start: Starting point of the method.
2. Input Image: Digital images in RGB or grayscale format are used as system input.
3. Resize Image to M x M: The image is resized to 256 × 256 pixels. This stage aims to: standardize the image size, fulfill the requirements of Arnold's Cat Map which requires the image to be square (square image).
4. ACM Encryption Fixed Iteration = 5: Arnold's Cat Map is applied to permute pixel positions. This process is repeated for 5 fixed iterations, according to the implementation in the source code. This stage aims to eliminate spatial correlation between pixels by randomizing pixel positions
5. Henon Map Diffusion XOR-based Subtitution: The Henon Map generates a chaotic sequence based on the following parameters: $a = 1.4$, $b = 0.3$, and initial conditions $x_0 = 0.1$ and $y_0 = 0.1$. This chaotic sequence is then applied to the pixel values using the XOR operation. This process does not change the pixel positions, but only randomizes the pixel intensity values (pixel substitution).
6. Encrypted Image (Cipher Image): The result of the permutation process is a cipher image.
7. End: Ending point of the method.

Explanation of the method decryption flow metode Henon Map from figure 8:

1. Start: Starting point of the method.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

2. Encrypted Image: The result of the permutation process is a cipher image.
3. Inverse Arnold's Cat Map Fixed Iterations = 5: The permutation is reversed using the inverse ACM with 5 iterations.
4. Henon Map Decryption (XOR again): The XOR operation is reapplied using the same chaotic sequence.
5. Decrypted Image: The original image was successfully restored.
6. End: Ending point of the method.

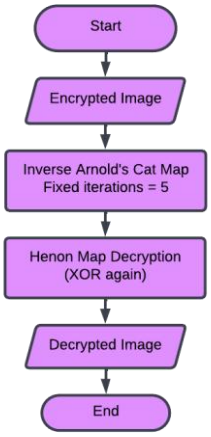


Figure 8. Arnold's Cat Map and Henon Map Decryption Flowchart

2.3.4. Henon Map and Arnold's Cat Map

In the Henon and ACM scheme, the resized image is first encrypted using the Henon map to perform pixel value diffusion through an XOR-based operation. The resulting image is then further encrypted using Arnold's Cat Map with five iterations to permute pixel positions. This scheme applies diffusion followed by confusion. The encryption and decryption procedures for this scheme are depicted in Figures 9 and 10.

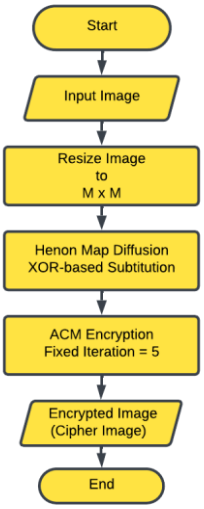


Figure 9. Henon Map and Arnold's Cat Map Encryption Flowchart

Explanation of method encryption flow Arnold's Cat Map from figure 9:

1. Start: Starting point of the method.
2. Input Image: Digital images in RGB or grayscale format are used as system input.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

3. Resize Image to M x M: The image is resized to 256 × 256 pixels. This stage aims to: standardize the image size, fulfill the requirements of Arnold's Cat Map which requires the image to be square (square image).
4. Henon Map Diffusion XOR-based Subtitution: The Henon Map generates a chaotic sequence based on the following parameters: a = 1.4, b = 0.3, and initial conditions $x_0 = 0.1$ and $y_0 = 0.1$. This chaotic sequence is then applied to the pixel values using the XOR operation. This process does not change the pixel positions, but only randomizes the pixel intensity values (pixel substitution).
5. ACM Encryption Fixed Iteration = 5: Arnold's Cat Map is applied to permute pixel positions. This process is repeated for 5 fixed iterations, according to the implementation in the source code. This stage aims to eliminate spatial correlation between pixels by randomizing pixel positions
6. Encrypted Image (Cipher Image): The result of the permutation process is a cipher image.
7. End: Ending point of the method

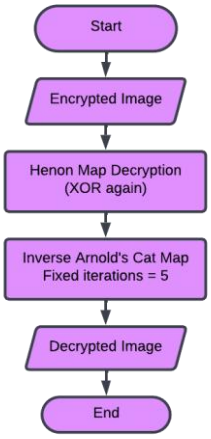


Figure 10. Henon Map and Arnold's Cat Map Decryption Flowchart

Explanation of the method decryption flow metode Henon Map from figure 10:

1. Start: Starting point of the method.
2. Encrypted Image: The result of the permutation process is a cipher image.
3. Henon Map Decryption: The XOR operation is reapplied using the same chaotic sequence.
4. Inverse Arnold's Cat Map Fixed Iterations = 5: The permutation is reversed using the inverse ACM with 5 iterations.
5. Decrypted Image: The original image was successfully restored.
6. End: Ending point of the method

2.4. Method Validation

Method validation focuses on measuring the quality of encryption results using several standard parameters, as shown in Figure 11.

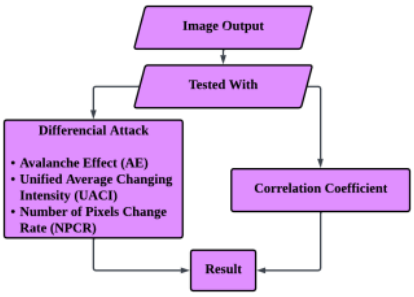


Figure 11. Method validation parameters

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

The Based on the evaluation metrics defined in Equations (1)–(4), the encryption performance can be interpreted using commonly accepted benchmark values reported in recent chaos-based image encryption studies [1], [6]. For the Avalanche Effect (AE) calculated using Equation (1), an ideal value is approximately 50%, indicating high sensitivity of the encryption algorithm to small changes in the plaintext image [35], [42]. Values approaching this threshold suggest strong diffusion characteristics and robustness against differential attacks [37], [43].

For the Number of Pixel Change Rate (NPCR) obtained from Equation (2), values greater than 99% are generally considered indicative of strong resistance to differential attacks in 8-bit image encryption schemes [1], [36], [43]. Similarly, the Unified Average Changing Intensity (UACI), computed using Equation (3), ideally approaches 33%, reflecting significant average intensity variation between cipher images generated from slightly different plaintexts [36], [43]. Although practical implementations may yield lower values, higher UACI values still indicate better diffusion capability [1], [11].

The pixel correlation coefficient calculated using Equation (4) is used to evaluate the statistical dependency between adjacent pixels in the encrypted image. Correlation values close to zero in the horizontal, vertical, and diagonal directions indicate the effective elimination of spatial correlation and strong resistance to statistical attacks [6], [11], [42]. These benchmark interpretations enable an objective evaluation of encryption quality without redefining the underlying mathematical formulations.

2.5. Method Analysis

The proposed image encryption methods are analyzed based on the fundamental principles of confusion and diffusion commonly adopted in chaos-based cryptographic systems. Arnold's Cat Map (ACM) primarily provides spatial permutation of pixels, which effectively disrupts the positional correlation in the image. However, as ACM does not modify pixel intensity values, its diffusion capability is inherently limited.

In contrast, the Hénon Map focuses on altering pixel intensity values through chaotic sequences, thereby enhancing diffusion and increasing randomness in the encrypted image. Nevertheless, without an explicit permutation stage, residual spatial dependency may remain.

The combined encryption schemes integrate both confusion and diffusion mechanisms to improve overall security. The order of combination plays a crucial role in determining the effectiveness of encryption. Applying diffusion before confusion is expected to intensify intensity variation before spatial permutation, while applying confusion first is scheduled to decorrelate pixel positions before modifying their values. These different operational sequences form the basis for comparative evaluation, which is further discussed in the Results and Discussion sections.

3. RESULT

This section presents the implementation and evaluation results of the Arnold's Cat Map and Henon Map encryption methods on various digital image formats, namely JPG, PNG, BMP, WEBP, and TIFF. The evaluation was carried out for each method individually and in two-way combinations, namely ACM→Henon and Henon→ACM. Encryption performance assessment was carried out based on the parameters Avalanche Effect (AE), Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), and Correlation Coefficient.

3.1. Encryption and Visualization results

This study uses the classic image "Lena" as one of the test objects. Figures 3, 5, 7, and 9 show the results of image encryption using four methods: Arnold's Cat Map (ACM), Henon Map, the combination

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

of ACM→Henon, and Henon→ACM. Meanwhile, Figures 4, 6, 8, and 10 show the decryption results of each method.

1. Arnold's Cat Map

Figure 12 below shows a visualization of the lena.jpg image resulting from the encryption and decryption process using the Arnold's Cat Map method.

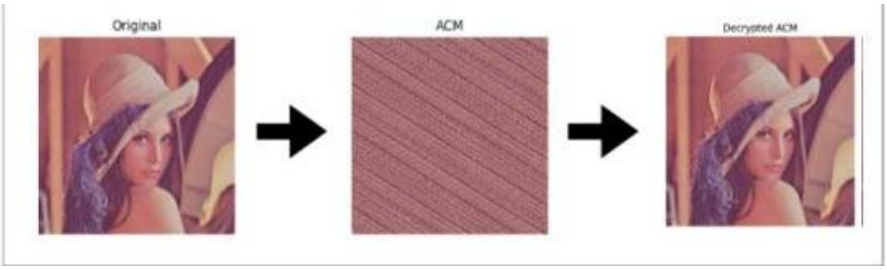


Figure 12. Arnold's Cat Map Method

Figure 12 above shows the results of a typical diagonal pattern that still retains some traces of the original image structure. This is because this method only permutates pixel positions (confusion), without changing the pixel intensity values. After the encryption and decryption processes, the encryption evaluation results were obtained using the parameters previously defined in Table 2 below.

Table 2. Evaluate calculations arnold's cat map

Entropy	6.8295
NPCR	99.13%
UACI	15.06%
Correlation (total)	-0.0015
Correlation (horizontal)	0.1252
Correlation (vertical)	-0.0086
Correlation (diagonal)	0.1745
Avalanche Effect	49.83%

Encryption of Lena.JPG with Arnold's Cat Map (ACM) shows effective pixel randomization. Entropy 6.8295 and NPCR 99.13% indicate randomness, but UACI 15.06% remains low as ACM does not alter intensity values. Pixel correlations were near zero, and the Avalanche Effect of 49.83% was close to ideal. Overall, ACM obscures image structure effectively but is less optimal for intensity distribution.

2. Henon Map

Figure 13 below shows a visualization of the lena.jpg image resulting from the encryption and decryption process using the Henon Map method.

Figure 13. Henon Map Method

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

Figure 13 above shows that Henon Map produces more random results than ACM because this method focuses on changes in pixel values (diffusion). After the encryption and decryption processes, the encryption evaluation results were obtained using the parameters previously determined in Table 3 below.

Table 3. Evaluate calculations Henon map

Entropy	7.9874
NPCR	98.15%
UACI	16.56%
Correlation (total)	0.1414
Correlation (horizontal)	-0.0641
Correlation (vertical)	0.0208
Correlation (diagonal)	0.0213
Avalanche Effect	47.93%

In the Henon Map method, the encryption from Lena.jpg results show a high level of randomness with an entropy value of 7.9874, which is close to the theoretical maximum value for 8-bit images. This indicates that the Henon Map is effective in changing pixel intensity values through a diffusion mechanism. However, the obtained NPCR value of 98.15% and UACI of 16.56% are still below the ideal value for resistance to differential attacks. In addition, the total correlation value of 0.1414 indicates that there is still spatial dependence between pixels in the cipher-image. This condition is understandable because the Henon Map only changes pixel values without permuting positions, so some of the spatial structure of the original image can still be detected statistically.

3. Arnold's Cat Map and Henon Map

Figure 14 below shows a visualization of the lena.jpg image resulting from the encryption and decryption process using the Arnold's Cat Map and Henon Map methods.

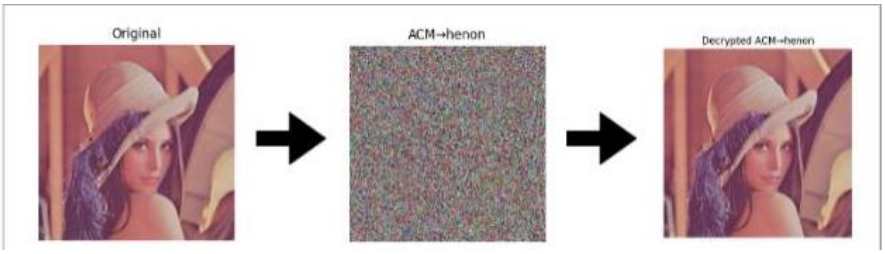


Figure 14. Arnold's Cat Map and Henon Map method

Figure 14 above shows that ACM→Henon produces a highly random cipher image with no detectable visual patterns, demonstrating the strength of the combination of confusion and diffusion, respectively. After the encryption and decryption processes, the encryption evaluation results were obtained using the previously defined parameters in Table 4 below.

Table 4. Evaluate calculations ACM and Henon

Entropy	7.9876
NPCR	99.44%
UACI	19.84%
Correlation (total)	0.0013
Correlation (horizontal)	-0.0010
Correlation (vertical)	0.0020
Correlation (diagonal)	0.0085
Avalanche Effect	50.01%

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

The combination of Arnold's Cat Map and Henon Map (ACM→Henon) significantly improved encryption quality compared to using the Henon Map alone. The entropy value increased to 7.9876, while the NPCR reached 99.44%, indicating that a single pixel change in the original image causes changes in almost all pixels in the cipher image. The UACI value also increased to 19.84%, indicating improved intensity diffusion, although it still fell short of the theoretical ideal value. All correlation coefficients in the horizontal, vertical, and diagonal directions were very close to zero, indicating that the statistical relationship between pixels was successfully eliminated. This improvement proves that the application of the confusion mechanism through ACM before Henon Map diffusion is able to strengthen the statistical security of encrypted images.

4. Henon Map and Arnold's Cat Map

Figure 15 below shows a visualization of the lena.jpg image resulting from the encryption and decryption process using the Arnold's Cat Map and Henon Map methods.

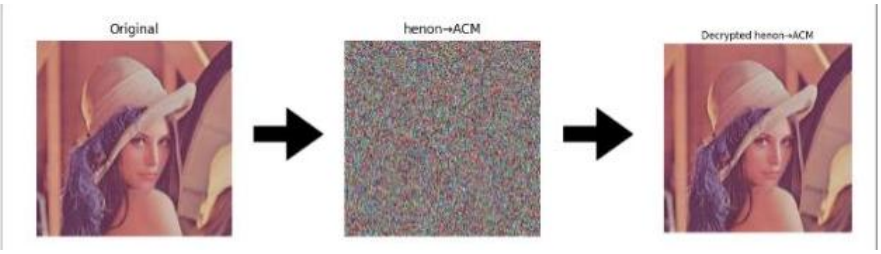


Figure 15. Henon Map and Arnold's Cat Map Method

Figure 15 above shows that Henon→ACM also produces a high degree of randomness, but different transformation sequences can affect the final structure of the random pixel distribution. After the encryption and decryption processes, the encryption evaluation results were obtained using the parameters previously determined in Table 5 below.

Table 5. Evaluate calculations Henon and ACM

Entropy	7.9874
NPCR	99.44%
UACI	19.93%
Correlation (total)	-0.0058
Correlation (horizontal)	-0.0007
Correlation (vertical)	-0.0000
Correlation (diagonal)	0.0007
Avalanche Effect	50.12%

The best results were obtained with the combination of Henon Map and Arnold's Cat Map (Henon→ACM). In this scheme, the entropy value reached 7.9874 and the NPCR was 99.44%, indicating a very high level of randomness and sensitivity to pixel changes. The UACI value of 19.93 was the highest compared to other methods in this study, while the Avalanche Effect value reached 50.12%, approaching the ideal value for a strong cryptographic system. All correlation coefficient values were very close to zero in all directions, indicating that spatial dependencies between pixels were effectively removed. The sequence of diffusion first using Henon Map, followed by permutation of pixel positions using ACM, proved to be more optimal in breaking the structural linkages of the image and producing a more random pixel distribution than the reverse sequence.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

3.2. Encryption Quality Analysis

The encryption quality analysis was conducted by comparing the performance of four encryption schemes, namely Arnold's Cat Map (ACM), Henon Map, the ACM→Henon combination, and the Henon→ACM combination, using entropy, NPCR, UACI, Avalanche Effect, and pixel correlation coefficients as evaluation metrics. The results indicate that both the type of chaotic mechanism and the order in which confusion and diffusion are applied have a significant impact on encryption strength.

The **ACM-only** scheme performs pixel position permutation (confusion) without modifying pixel intensity values. As a result, it is effective in reducing spatial correlation between pixels but produces a relatively low UACI value due to the absence of diffusion. In contrast, the **Henon Map-only** scheme focuses on pixel value diffusion and achieves entropy values close to the theoretical maximum for 8-bit images. However, without a permutation stage, the Henon Map still exhibits residual spatial dependency, as reflected by a relatively higher total correlation coefficient compared to the combined schemes.

A substantial improvement in encryption quality is observed when confusion and diffusion are combined. The **ACM→Henon** scheme demonstrates that applying permutation prior to diffusion increases NPCR to 99.44% and reduces pixel correlation values to nearly zero in all directions. The Avalanche Effect approaches the ideal value of 50%, indicating high sensitivity to small changes in the plaintext image. Nevertheless, the obtained UACI value remains below the theoretical ideal, suggesting that intensity diffusion is improved but not yet optimal.

Among all evaluated methods, the **Henon→ACM** scheme achieves the best overall performance. Applying diffusion first using the Henon Map, followed by confusion through Arnold's Cat Map, results in the most effective elimination of spatial structures in the cipher image. This scheme produces an entropy value of 7.9874, an NPCR of 99.44%, the highest UACI among the tested methods, and an Avalanche Effect of 50.12%. Moreover, pixel correlation coefficients in the horizontal, vertical, and diagonal directions are all very close to zero, indicating that linear dependencies between neighboring pixels have been effectively removed.

Based on both the experimental results and findings reported in related chaos-based image encryption studies, it can be concluded that the **Henon→ACM combination is the most optimal method** in this research. The diffusion-first and confusion-second sequence provides stronger randomness, higher sensitivity, and better resistance to statistical attacks than single-map encryption or the reverse combination order. Although the UACI values obtained are still below the theoretical ideal, the overall evaluation metrics confirm that the Henon→ACM scheme offers the strongest and most stable encryption quality among the methods examined.

4. DISCUSSIONS

The experimental results demonstrate that combining Arnold's Cat Map (ACM) and Henon Map significantly enhances image encryption quality compared to using each chaotic map independently. This improvement is consistently reflected across multiple evaluation metrics, including entropy, NPCR, UACI, Avalanche Effect, and pixel correlation coefficients. The obtained entropy values for the combined schemes (≈7.99) are very close to the theoretical maximum for 8-bit images, indicating a near-uniform distribution of pixel intensities in the encrypted images [37], [43] .

When the chaotic maps are applied individually, their limitations become evident. The ACM-only scheme performs pixel permutation without modifying intensity values, which effectively reduces spatial correlation but results in limited diffusion capability, as indicated by the relatively low UACI value. Conversely, the Henon Map-only scheme provides strong diffusion at the pixel-value level and achieves high entropy; however, without a permutation stage, residual spatial dependency remains in the encrypted image, as reflected by higher pixel correlation values. Similar limitations of confusion-

only and diffusion-only schemes have also been reported in previous chaos-based image encryption studies [11], [20].

The combination schemes demonstrate that integrating confusion and diffusion mechanisms is essential for robust image encryption. In both ACM→Henon and Henon→ACM configurations, pixel correlation values are reduced to nearly zero in the horizontal, vertical, and diagonal directions, while NPCR values approach those required for strong resistance against differential attacks. This observation is consistent with prior research emphasizing the importance of confusion–diffusion integration in chaos-based cryptosystems [11], [31], [42].

Among all tested configurations, the Henon→ACM scheme yields the best overall performance. Applying diffusion first using the Henon Map ensures that pixel intensity values are thoroughly randomized, while the subsequent ACM permutation disrupts the spatial relationships among pixels more effectively than the reverse order. This diffusion-first strategy has been shown in recent studies to enhance resistance against statistical and differential attacks by minimizing residual spatial structures in the cipher image [11], [15], [20].

Although the combined schemes significantly improve encryption performance, the obtained UACI values (≈19–20%) remain below the theoretical ideal of approximately 33% for fully randomized 8-bit cipher images. Similar observations have been reported in related studies, where strong confusion and diffusion mechanisms still require additional rounds or adaptive chaotic parameters to achieve ideal UACI levels [37], [43]. This limitation suggests potential directions for future work, such as increasing diffusion iterations or incorporating additional chaotic maps.

Overall, the discussion confirms that the proposed Henon→ACM scheme achieves a favorable balance between randomness, sensitivity, and statistical security. While not reaching the theoretical optimum in all metrics, it outperforms the single-map and reverse-order combination schemes, making it a robust and effective approach for chaos-based image encryption.

5. CONCLUSION

This study has evaluated the encryption quality of digital images using Arnold's Cat Map (ACM) and Henon Map algorithms, applied individually and in two different combination sequences, namely ACM→Henon and Henon→ACM. The evaluation was conducted on multiple image formats using standard statistical and differential attack metrics, including entropy, NPCR, UACI, Avalanche Effect, and pixel correlation coefficients.

The experimental results show that single-map encryption schemes exhibit inherent limitations. The ACM-only method effectively reduces spatial correlation through pixel permutation but provides limited diffusion, resulting in low UACI values. Conversely, the Henon Map-only method achieves high entropy by modifying pixel intensity values but still retains residual spatial dependency due to the absence of pixel position permutation. These findings confirm that neither confusion-only nor diffusion-only approaches are sufficient to achieve optimal image encryption security.

A significant improvement is observed when confusion and diffusion mechanisms are combined. Both combined schemes successfully reduce pixel correlation to near zero and increase resistance to differential attacks. Among all tested configurations, the Henon→ACM scheme demonstrates the best overall performance, achieving entropy values close to the theoretical maximum, NPCR values of approximately 99.44%, the highest UACI among the evaluated methods, and an Avalanche Effect close to the ideal 50%. The diffusion-first and confusion-second sequence proves to be more effective in disrupting pixel intensity patterns and spatial structures than the reverse order.

Although the combined schemes significantly enhance encryption quality, the obtained UACI values remain below the theoretical ideal for fully randomized 8-bit images, indicating that further improvements in diffusion strength are still possible. Future research may focus on adaptive parameter

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

optimization, increased diffusion iterations, or the integration of additional chaotic maps to further enhance intensity variation and resistance to differential attacks. Overall, this study confirms that the Henon→ACM configuration offers a robust and effective solution for chaos-based image encryption across multiple image formats

ACKNOWLEDGEMENT

The author expresses gratitude to Diponegoro University for its assistance and to the research team and lecturers who have contributed constructive criticism and technical advice that has significantly raised the caliber of this study.

REFERENCES

[1] H. Zhang, X. Feng, J. Sun, and P. Yan, "Chaotic Image Security Techniques and Developments: A Review," *Mathematics*, vol. 13, pp. 1–28, Jun. 2025, doi: 10.3390/math13121976.

[2] M. Jiang and H. Yang, "Image Encryption Using a New Hybrid Chaotic Map and Spiral Transformation," *Entropy*, vol. 25, pp. 1–18, Nov. 2023, doi: 10.3390/e25111516.

[3] L. Li, "A novel chaotic map application in image encryption algorithm," *Expert Syst Appl*, vol. 252, May 2024, doi: 10.1016/j.eswa.2024.124316.

[4] Y. Yang, J. Gao, and H. Imani, "Design, analysis, circuit implementation, and synchronization of a new chaotic system with application to information encryption," *AIP Adv*, vol. 13, Jul. 2023, doi: 10.1063/5.0161382.

[5] P. S. Sneha, S. Sankar, and A. S. Kumar, "A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps," *J Ambient Intell Humaniz Comput*, vol. 11, no. 3, pp. 1289–1308, Mar. 2020, doi: 10.1007/s12652-019-01385-0.

[6] A. Dinu and M. Frunzete, "Image Encryption Using Chaotic Maps: Development, Application, and Analysis," vol. 13, pp. 1–16, Aug. 2025, doi: 10.3390/math13162588.

[7] D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," *Applied Sciences (Switzerland)*, vol. 13, no. 12, Jun. 2023, doi: 10.3390/app13127113.

[8] A. Arham and N. Lestari, "Secure medical image watermarking based on reversible data hiding with Arnold's cat map," *International Journal of Advances in Intelligent Informatics*, vol. 9, no. 3, pp. 445–456, Nov. 2023, doi: 10.26555/ijain.v9i3.1029.

[9] V. Rathore and A. K. Pal, "An image encryption scheme in bit plane content using Henon map based generated edge map," *Multimed Tools Appl*, vol. 80, no. 14, pp. 22275–22300, Jun. 2021, doi: 10.1007/s11042-021-10719-0.

[10] K. V. Sudheesh, S. B. Santhosha, and K. Puttegowda, "Henon Maps based selective image encryption approach for enhanced control and security," *Journal of Integrated Science and Technology*, vol. 13, no. 2, 2025, doi: 10.62110/sciencein.jist.2025.v13.1034.

[11] 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.

[12] Q. K. Abed and W. A. M. Al-Jawher, "Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm," *Journal Port Science Research*, vol. 7, no. 3, Jul. 2024, doi: 10.36371/port.2024.3.3.

[13] A. Musthofa, D. Rosal, and I. M. Setiadi, "Layered Image Encryption Method Based on Combination of Logistic Map, Henon Map, and Sine Map to Enhance Digital Image Security," *Journal of Applied Informatics and Computing (JAIC)*, vol. 9, no. 4, pp. 1280–1289, Aug. 2025, doi: 10.30871/jaic.v9i4.9569.

[14] Siti Nurul Hatikah Mohammad and Arif Mandangan, "Colour Image Encryption and Decryption using Arnold's Cat Map and Henon Map," *International Journal of Advanced Research in Computational Thinking and Data Science*, vol. 1, no. 1, pp. 41–52, Apr. 2025, doi: 10.37934/ctds.1.1.4152a.

[15] M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A new color image encryption algorithm using multiple chaotic maps with the intersecting planes method," *Sci Afr*, vol. 16, Jul. 2022, doi: 10.1016/j.sciaf.2022.e01217.

[16] U. Zia *et al.*, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int J Inf Secur*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[17] A. Tiwari, P. Diwan, T. D. Diwan, M. Miroslav, and S. P. Samal, "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication," *Sci Rep*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-95995-8.

[18] S. Kanwal, S. Inam, S. Al-Otaibi, J. Akbar, N. Siddiqui, and M. Ashiq, "An efficient image encryption algorithm using 3D-cyclic chebyshev map and elliptic curve," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-77955-w.

[19] W. Lu, C. Jin, J. Wang, X. Liu, J. Liu, and Z. Zhai, "A novel image encryption scheme using 3D chaotic maps with Josephus permutation and dynamic diffusion," *Journal of King Saud University - Computer and Information Sciences*, vol. 37, no. 8, Oct. 2025, doi: 10.1007/s44443-025-00284-z.

[20] M. Mohammed Ibrahim and R. Venkatesan, "Image encryption using novel chaotic map and cellular automata dynamics," *RAIRO - Theoretical Informatics and Applications*, vol. 59, p. 2, 2025, doi: 10.1051/ita/2025001.

[21] K. M. Hosny, Y. M. Elnabawy, R. A. Salama, and A. M. Elshewey, "Multiple image encryption algorithm using channel randomization and multiple chaotic maps," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-79282-6.

[22] M. A. Alkhonaini, E. Gemeay, F. M. Zeki Mahmood, M. Ayari, F. A. Alenizi, and S. Lee, "A new encryption algorithm for image data based on two-way chaotic maps and iterative cellular automata," *Sci Rep*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-64741-x.

[23] R. Vinoth Raj, V. Vinoth Kumar, R. Murugan, and K. Yazhini, "5D chaotic map-based image encryption trade-off analysis on various stages of encryption," *EURASIP J Adv Signal Process*, vol. 2025, no. 1, Dec. 2025, doi: 10.1186/s13634-025-01255-2.

[24] S. Subathra and V. Thanikaiselvan, "Image adaptive encryption using EfficientNet B3 feature guided multi scroll chaotic map with modulo controlled pseudo parallel processing," *Sci Rep*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-27080-z.

[25] A. Y. Darani, Y. K. Yengejeh, H. Pakmanesh, and G. Navarro, "Image encryption algorithm based on a new 3D chaotic system using cellular automata," *Chaos Solitons Fractals*, vol. 179, Feb. 2024, doi: 10.1016/j.chaos.2023.114396.

[26] M. Aliyu, O. F. Nonso, A. Abdullahi, U. Sani, and Z. L. Hassan, "Secure document and image transmission through an encrypted network system," *Dutse Journal of Pure and Applied Sciences*, vol. 8, no. 3b, pp. 1–14, Oct. 2022, doi: 10.4314/dujopas.v8i3b.1.

[27] R. Risna, Y. Amaliah, and S. Yunita, "Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Cipher," *Sebatik*, vol. 26, no. 2, pp. 525–534, Dec. 2022, doi: 10.46984/sebatik.v26i2.2061.

[28] H. Fan, C. Zhang, H. Lu, M. Li, and Y. Liu, "Cryptanalysis of a new chaotic image encryption technique based on multiple discrete dynamical maps," *Entropy*, vol. 23, no. 12, pp. 1–17, Dec. 2021, doi: 10.3390/e23121581.

[29] X. Wang, S. Chen, and Y. Zhang, "A chaotic image encryption algorithm based on random dynamic mixing," *Opt Laser Technol*, vol. 138, pp. 2–17, Jun. 2021, doi: 10.1016/j.optlastec.2020.106837.

[30] T. Adi Putra, I. Ruslianto, and S. Bahri, "Penerapan Metode Arnold Cat Map dan Logistic Map untuk Pengamanan Citra Data Penduduk," *Journal of Computing Engineering, System and Science*, vol. 2, pp. 470–481, Jul. 2022, doi: 10.24114/cess.v7i2.36302.

[31] M. Gupta, S. Bhattacharjee, and B. Chatterjee, "An Enhanced Security in Medical Image Encryption Based on Multi-level Chaotic DNA Diffusion," *Journal of Image and Graphics(United Kingdom)*, vol. 11, no. 2, pp. 153–160, Jun. 2023, doi: 10.18178/joig.11.2.153-160.

Vol. 7, No. 3, June 2026, Page. 2225-2245
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.3.5354

[32] A. Sabah, S. Hameed, and M. A. A. K., "Key Generation based on Henon map and Lorenz system," *Al-Mustansiriyah Journal of Science*, vol. 31, no. 1, pp. 41–46, Mar. 2020, doi: 10.23851/mjs.v31i1.734.

[33] S. Kanwal *et al.*, "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices," *Sensors*, vol. 22, no. 12, Jun. 2022, doi: 10.3390/s22124359.

[34] M. A. Islam, I. R. Hassan, and P. Ahmed, "Dynamic complexity of fifth-dimensional Henon map with Lyapunov exponent, permutation entropy, bifurcation patterns and chaos," *J Comput Appl Math*, vol. 466, Oct. 2025, doi: 10.1016/j.cam.2025.116547.

[35] Muslih and L. B. Handoko, "Pengujian Avalanche Effect Pada Kriptografi Teks Menggunakan Autokey Cipher," *2 st Proceeding STEKOM*, vol. 2, no. 1, pp. 127–134, Dec. 2022, doi: 10.51903/semnastekmu.v2i1.162.

[36] R. Saidi, N. Cherrid, T. Bentahar, H. Mayache, and A. Bentahar, "Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted inSAR interferogram," *Ingenierie des Systemes d'Information*, vol. 25, no. 5, pp. 601–607, Nov. 2020, doi: 10.18280/ISI.250507.

[37] S. A. Mehdi and Z. latif Ali, "Image Encryption Algorithm Based on a Novel Six-Dimensional Hyper- Chaotic System," *Al-Mustansiriyah Journal of Science*, vol. 31, no. 1, pp. 54–63, Mar. 2020, doi: 10.23851/mjs.v31i1.739.

[38] S. M. Kareem and A. M. S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102410.

[39] H. Djamel, H. Abdarrahmane, I. Haddad, B. Aïssa, N. Derouiche, and H. Kahia, "An Algorithm for Image encryption based on chaotic maps," *ICMAR*, vol. 1, pp. 110–118, Aug. 2023.

[40] S. S. Nurhaliza and L. ETP, "Sistem Pengenalan Karakter Dokumen Secara Otomatis Menggunakan Metode Optical Character Recognition," *PETIR*, vol. 15, no. 1, pp. 166–175, Mar. 2022, doi: 10.33322/petir.v15i1.1610.

[41] W. Alexan *et al.*, "A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5," *Sci Rep*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-92065-x.

[42] A. N. Latifa, C. A. Sari, E. H. Rachmawanto, and M. K. Sarker, "Multi-Level Secure Image Cryptosystem Using Logistic Map Chaos: Entropy, Correlation, and 3D Histogram Validation," *Jurnal Masyarakat Informatika*, vol. 16, no. 2, pp. 247–267, Nov. 2025, doi: 10.14710/jmasif.16.2.74537.

[43] Z. A. N. Fauzyah, A. Nugraha, A. Luthfiarta, and M. N. E. Farandi, "An Enhanced Multi-Layered Image Encryption Scheme Using 2d Hyperchaotic Cross-System And Logistic Map With Route Transposition," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 1, pp. 11–22, Feb. 2025, doi: 10.52436/1.jutif.2025.6.1.4007.