Enhanced Image Encryption through Combined Arnold and Three Other Chaos Techniques

Sameeh Abdulghafour Jassim[1,2,*], Alaa Abulqahar Jihad[3], Mohammed I. Khalaf[2,*]

[1]Department of Vocational Education in Anbar, Ministry of Education, Anbar, Iraq

[2]Department of Computer Sciences, College of Science, University of Al Maarif, Al Anbar, 31001, Iraq

[3] Computer Center, University of Anbar, Al Anbar,31001, Iraq

Emails: sameeh@uoa.edu.iq; it.alaa.heety@uoanbar.edu.iq; m.i.khalaf@uoa.edu.iq

Abstract

In an era where digital technologies dominate all aspects of life, image encryption has emerged as a fundamental pillar of data protection and securing sensitive information. With the rise of sophisticated cyber threats and attacks, the search for innovative and stronger encryption methods has become an urgent necessity. This research proposes an enhanced image encryption scheme combining the Arnold map, 2D Henon map, memristor elements, and exponential nonlinearity chaos techniques to address vulnerabilities in conventional encryption methods. The hybrid approach ensures robustness against statistical, differential, and brute-force attacks. Experimental results demonstrate superior performance with unified histogram distribution, including near-ideal information entropy (7.99941), infinite peak signal-to-noise ratio (PSNR), and high resistance to differential attacks (NPCR = 99.61%, UACI = 35.08%). A keyspace of 2^{2460} and key sensitivity correlation difference rate (CDR) of 99.61% further validate security. Comparative analysis with recent studies confirms the proposed method's superiority in encryption strength and computational performance. Consequently, the results of the proposed method making it a promising option for high-security image protection applications.

Keywords: Security; Cryptography; Chaos system; Cipher image

1. Introduction

In our digital era, securing multimedia data, especially images, has become increasingly critical due to the widespread use of images in various fields such as military, medical, finance, and personal communication. Therefore, digital image encryption is becoming critical for securing sensitive data. However, traditional algorithms (e.g., AES, DES, and RSA) struggle with high redundancy and strong pixel correlation inherent in images. Chaos-based encryption has emerged as a promising alternative owing to its high sensitivity to initial conditions and pseudorandom behavior[1]. Recent studies leverage 2D chaotic maps (e.g., Arnold and Henon) for pixel scrambling and diffusion[2]. However, standalone chaos systems often exhibit periodicity or limited keyspaces, making them vulnerable to brute-force and differential attacks. To overcome these limitations, researchers have integrated memristors for dynamic key generation and exponential nonlinearity to enhance chaotic complexity.

This work introduces a novel hybrid framework combining the Arnold map for pixel permutation, the 2D Henon map for diffusion, memristor-based key modulation, and exponential nonlinearity chaos to amplify unpredictability. The integration addresses individual component weaknesses while achieving high security and efficiency. Experiments validate the method's resistance to statistical, differential, and key-based attacks, outperforming recent schemes[3]. Moreover, the proposed method can implement in cloud computing[4][5], to provide a secure way to store and transmit sensitive image data, leveraging the cloud's scalability and processing power to handle the computational demands of these encryption algorithms.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

This paper is structured as follows: Section 2 reviews the existing literature on image encryption. Section 3 details the fundamental components of the encryption algorithm, including the 2D Henon map, a memristor element, a chaotic system with exponential nonlinearity, and the Arnold transformation, providing the necessary background for understanding the system's dynamics. Section 4 presents the proposed hybrid encryption method, outlining the specific steps and integrations of these chaotic elements. Section 5 displays the results obtained from applying the proposed method, including comparisons with existing techniques to demonstrate its effectiveness and security. Finally, Section 6 concludes the paper by summarizing the key findings and exploring potential avenues for future research.

2. Related Works

Modern image encryption employs a wide range of approaches, including those based on chaotic systems, optimization algorithms, and combined methods. While these approaches demonstrate promising results, critical limitations persist, as discussed below:

Chaotic Systems and Multi-Stage Optimization: Several studies, such as [6] and [7], rely on chaotic systems combined with optimization algorithms to enhance security. The method in [6] employs block compressive sensing (BCS), Swin Transformers, and Wild Horse Optimization (WHO), achieving high NPCR (99.54%) and UACI (33.42%). However, the multi-stage workflow (including DWT, FAN transforms, and BCS) introduces computational overhead, limiting real-time applicability. Similarly, [7] combines Arnold transforms, URUK chaotic maps, and Grey Wolf Optimization (GWO) for color image encryption. While GWO improves pixel decorrelation, the Arnold transform's inherent periodicity risks predictability if iteration counts are not dynamically randomized. Furthermore, both [6] and [7] process RGB channels independently, neglecting inter-channel correlations, which could leave residual patterns exploitable by correlation-based attacks.

High-Dimensional Chaos and Decomposition Techniques: The 5D chaotic system in [8] and the modular discrete derivative (MDD) in [9] emphasize high-dimensional chaos and matrix decomposition for medical and color image encryption. In [8], QR decomposition and an improved Joseph loop enhance diffusion, but the computational complexity of decomposing large medical images (e.g., MRI/CT scans) may hinder scalability. Additionally, the Joseph loop's scrambling mechanism lacks empirical validation against known-plaintext attacks. Similarly, [9] integrates MDD with Langton's ant, achieving entropy >7.999 and NPCR >99.6%. However, MDD's mathematical novelty requires rigorous cryptanalysis to verify resistance to algebraic attacks. Langton's ant, while Turing-complete, exhibits deterministic behavior over iterations, which adversaries could exploit if partial key information is compromised.

Fractional-Order Systems and Hybrid Compression-Encryption: The fractional-order hyperchaotic system in [10] and the hybrid scheme in [11] explore advanced mathematical models. In [10], a fractional-order Chen system and Fibonacci Q-matrices achieve strong diffusion, but the computational complexity of fractional calculus limits practical deployment in resource-constrained devices. Block-wise diffusion using Fibonacci Q-matrices may also introduce fixed patterns if parameters are reused across encryption instances. Meanwhile, [11] integrates chaos-based permutation with lossless compression, improving compression rates by 15.45%. However, compressing shuffled images risks exposing residual statistical redundancies, undermining diffusion. The substitution stage's reliance on chaotic sequences may fail to mask patterns in compressed data, leaving vulnerabilities to entropy-based attacks.

Multi-Chaotic Key Generation and Validation Gaps: Studies like [12] and [9] utilize multiple chaotic maps (e.g., 2D Logistic Sine, Tent, Bernoulli) to generate keys. While [12] reports NIST SP 800 suite compliance, its reliance on four distinct chaotic systems complicates key management, potentially increasing vulnerability to brute-force attacks if key-space expansion is not rigorously validated. Similarly, [9]'s use of MDD and Langton's ant lacks empirical validation against adaptive chosen-ciphertext attacks.

In conclusion, despite achieving robust metrics, the reviewed methods exhibit critical weaknesses such as computational inefficiency in multi-stage workflows, security-compression trade-offs, etc. These limitations underscore the need for streamlined architectures and adversarial robustness testing that we will try to enhance them in the proposed work and then compare the analysis of the proposed work with existing approaches.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

3. Chaotic Map

Chaotic maps attained preeminence on the canvas of computer security largely because to the intrinsic characteristics of sensitivity to initial conditions, ergodicity, and unpredictability. These general properties can even be exploited for applications of encryption, random number generation, and secure communication[13]. In the following sections, specific chaotic maps shall be exploited, 2D Henon maps, memristor-based chaotic systems, chaotic systems with exponential nonlinearity, and Arnold transformations, in view of images security.

A. 2D Henon map

Michel Henon gave the name Henon when he introduced the map in 1976 and since then, it has adequately applied itself as the prime prototype for two-dimensional chaotic systems. In mathematical language, the Henon map is expressed by the two following equations[14]:

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

$$y_{n+1} = bx_n \quad (2)$$

Where *a* and *b* represent the system parameters. The classical chaotic behavior of the map sets in when a = 1.4 and b = 0.3 and produces the characteristic butterfly-shaped strange attractor. Figure 1. Shows the Henon map.

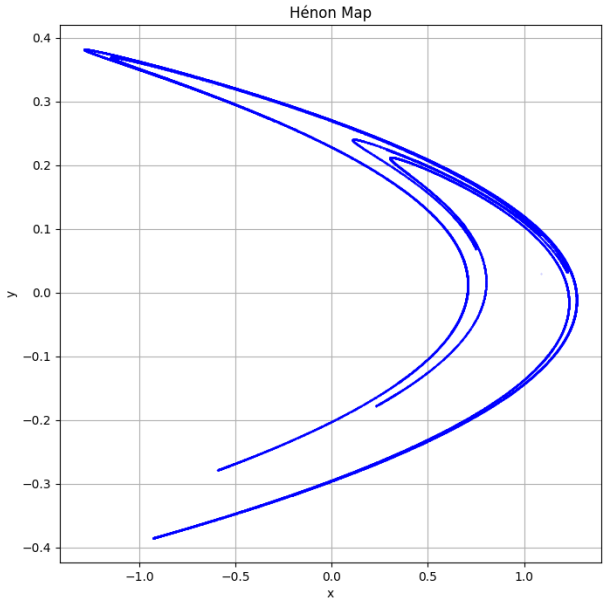

Figure 1. Henon map

Even well accepted, in most of the security implementations, limiting factors of the traditional Henon map are manifested. The most important among them is the fact that its chaotic regions are discontinuous and most times isolated, in such a way that negligible variation in control parameters may switch the system from chaotic to non-chaotic behavior. This is really a weakness for typical security applications that require the system to be consistently chaotic over a range of parameter values. Secondly, the output distribution is limited, as the trajectories are confined to a narrow region within the phase plane, featuring distinct and recognizable patterns. Henon map-based encryption schemes might become weak in this sense since with a smaller range of outputs, it is easier to break them statistically or cryptographically[15]. To address these limitations, more than one chaotic map will be combined.

B. Memristor element

The memristor in this proposed is described by the nonlinear function $M(x) = x^2$, a rather simplified form as compared to other and more complex memristor models, for example, the TEAM (ThrEshold Adaptive Memristor) model[16]. However, it captures the essential nonlinear behavior that defines memristive devices. The proposed system takes in the three classic equations of Lorenz (with some slight modifications) besides another equation that describes the state variable w of the memristor. The slight modifications that will be used in the implementation of a dynamical system of four dimensions will involve the combination of a modified classic

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

Lorenz chaotic system with an element of a memristor. This system will then be presented in a set of differential equations as follows:

$$\frac{dx}{dt} = a(y - x) - w.M(x) \quad (3)$$

$$\frac{dy}{dt} = bx - xz + cy \quad (4)$$

$$\frac{dz}{dt} = xy - dz \quad (5)$$

$$\frac{dw}{dt} = ex - fw \quad (6)$$

Where: $x, y, z, and\ w$ are the state variables. Whereas as $a, b, c, d, e, and\ f$ are the system parameters. Finally, $M(x) = x^2$ is the nonlinear memristor function. Additionally, the parameters used in the simulation was: a=10, b=28, c=2.7, d=e=f=1.

The memristor and the chaotic system, however, communicate in two ways:

1. The dynamics of the x variable are affected by the memristor state, w by the term $-w.M(x)$.
2. The x variable communicates to the memristor state through the term ex in the (4) uation.

This bidirectional coupling will create a pretty complex dynamical system, and of course rich behaviors also depend on the values of the parameters[17]. Moreover, to be able to understand the dynamics of the system, we shall implement visualizations in python code that will aid us in identifying chaotic attractors, and also try to see the influence of the memristor on the overall behavior. The code will output the following two main types of visualizations:

1. Time series plots: The evolution of each state variable over time is illustrated by four individual graphs. It is shown in Figure 2.
2. Phase space projections: Four plots that show the interrelationships between different pairs of variables. Specifically, it is x versus y, x versus z, y versus z, and x versus w. They are presented in Figure 3.
3.

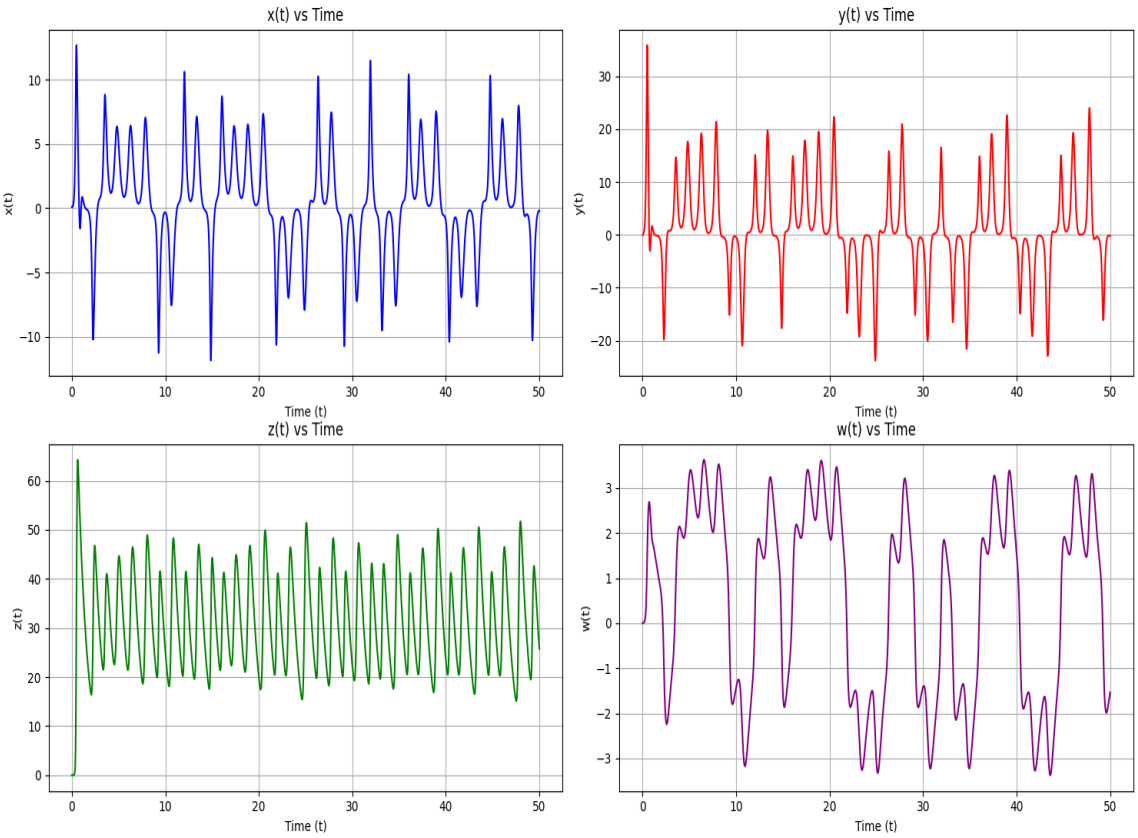

Figure 2. Time series plots

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

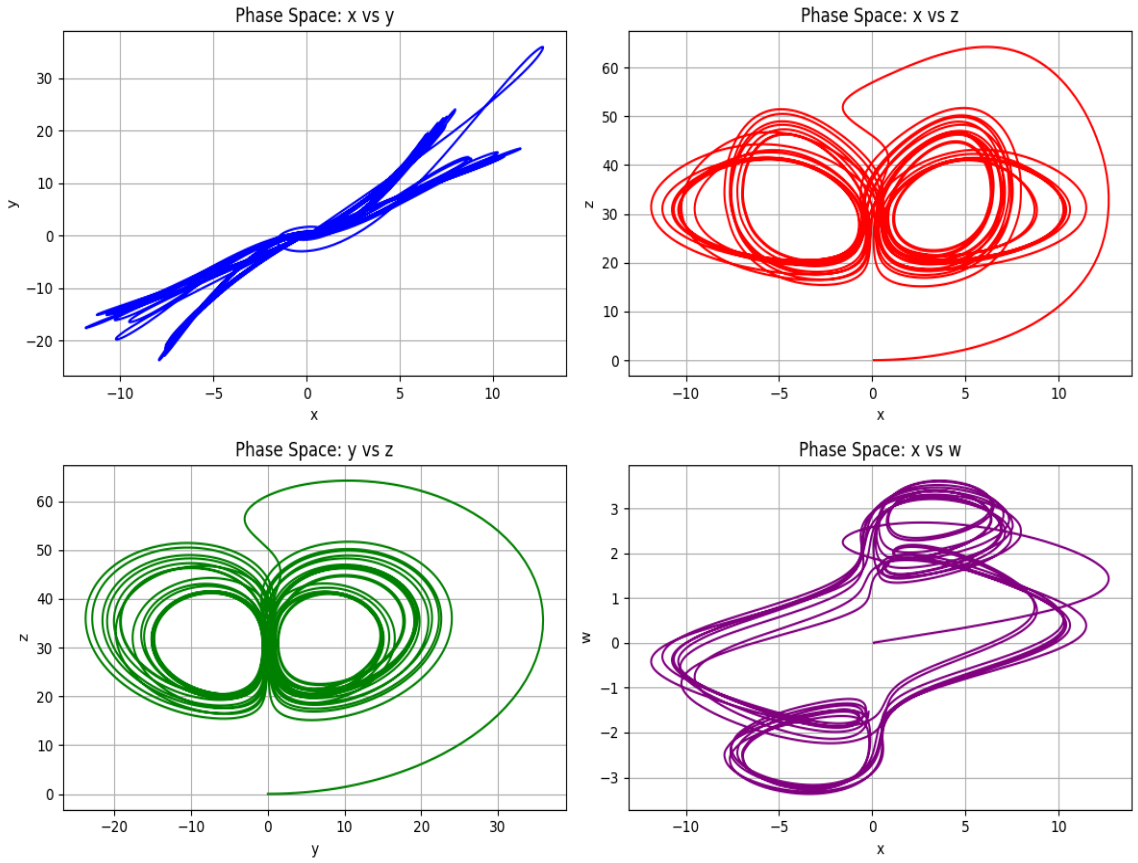

Figure 3. Phase space projections

C. Chaotic System with Exponential Nonlinearity

In this paper, we merged the modified Lorenz system with exponential nonlinearity. Compared to the classical chaotic systems, the exponential term provides additional bifurcation parameters that enable the attractor geometries to be more complex. Chaotic behavior was revealed in both numerical integration and phase space visualization. In our method, three coupled nonlinear differential equations are used for representation as an exponentially chaotic oscillator[18]:

$$\frac{dx}{dt} = a(x - y) \quad (7)$$

$$\frac{dy}{dt} = bx - xz + cy \quad (8)$$

$$\frac{dz}{dt} = xy - dz + e.e^{fx} \quad (9)$$

The default values of the parameters are: a=10, b=28, c=2.7 (Lorenz system parameters) and d=e=f=1 (Exponential term coefficients).

The key features of this method to inherits chaotic characteristics from the classical Lorenz system through the xy and xz terms. In addition, introduces exponential nonlinearity e^{fx} in the z-dynamics, creating additional system complexity. Figure 4. Shows the Time-Domain Plots and the 3D Phase Space Trajectory. The Time-Domain is used to help identify periodicity, divergence, or transient behavior. While the phase space is revealing the system's attractor structure, which is critical for analyzing chaos (for example, butterfly effect).

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

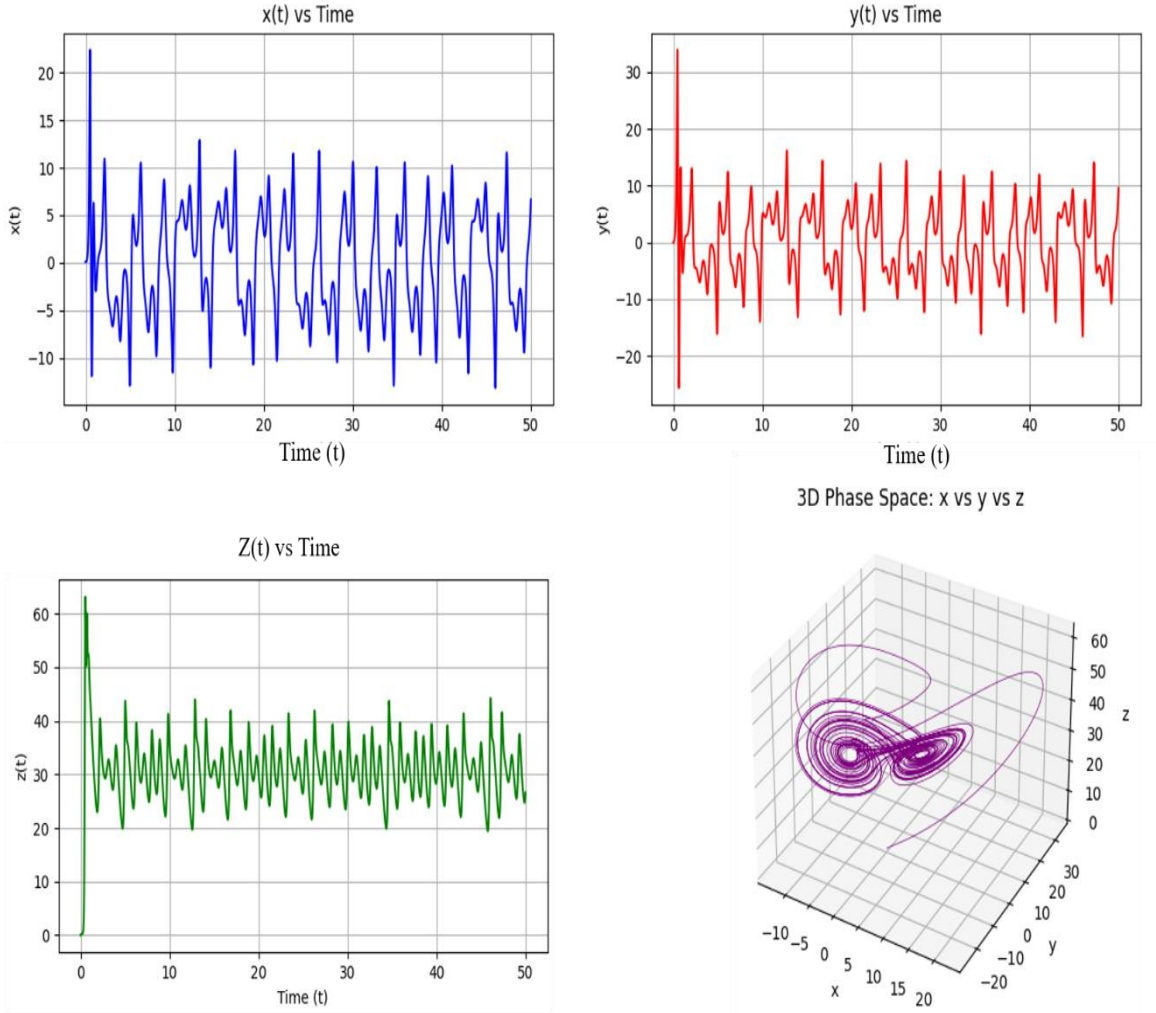

Figure 4. Time-Domain Plots and the 3D Phase Space Trajectory

D. Arnold Transformation

The Arnold transformation has been put forward as a very strong mathematical technique in data security since it offers very strong encryption through unorthodox properties. Another name by which it goes is Arnold's cat mapping since it scrambles data in a way that looks chaotic but is perfectly reversible under some rather strict conditions. Its applications range from image encryption to the broader scope of general data security protocols, and therefore it is a hot study subject in modern cryptography.

The Arnold transformation is a map that is chaotic and was first instituted by Vladimir Arnold in the proof of ergodic theory using the image of a cat. The Arnold transformation is defined as a linear transformation that maps the coordinates of a pixel in a square image to new coordinates. As described in[2], the basic Arnold transformation can be represented mathematically as a modulo function[19]:

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = A \begin{pmatrix} x_i \\ y_i \end{pmatrix} mod\ N \qquad (10)$$

Where (x_i, y_i) represents the original coordinates, (x_{i+1}, y_{i+1}) will represent the new coordinates after transformation, A is the key matrix, and N is the circumference number or image size. This transformation essentially "stretches and folds" the data in a manner similar to kneading dough, creating a scrambling effect that will make the original data unrecognizable.

The key matrix A is normally a 2×2 matrix with integer entries. The standard Arnold transformation uses[20]:

$$A=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad (11)$$

But for better security in modern applications, they use generalized Arnold transforms with changing parameters. The transformation's effectiveness in encryption stems from its unpredictable nature while maintaining perfect reversibility, a critical property for any encryption system that must allow for decryption.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

4. The proposed methods

In the area of computer security, encryption algorithms are most essential in securing the data. In which chaos-based one, has directly gained powers in visibility to the aspects of unpredictability, the system's sensitivity to initial conditions, along with its ergodicity. This section will introduce a new algorithm with 2D Henon map as a core chaotic system for generating secure encryption keys and indices for image encryption. In addition, this algorithm will use other chaotic maps to the memristor element and exponential nonlinearity beside the Arnold map to increase the strength and security of the encryption procedure. In addition, the integration of Arnold's cat map further enhances diffusion by scrambling pixel positions. Efficient image encryption and decryption have been proposed in this algorithm.

A. Image Collection and Preprocessing

Images are vulnerable to unauthorized access, theft, and tampering as they are transmitted over a network or stored. The privacy and integrity of images can be well preserved by image encryption, thus ensuring safe transmission and storage of data. Apart from those, the other advantages of image encryption include the prevention of illegal copying or piracy of images, thus protecting the copyright and commercial interests of the original images, and protecting the rights of image creators. Figure 5 shows the image data from[21].

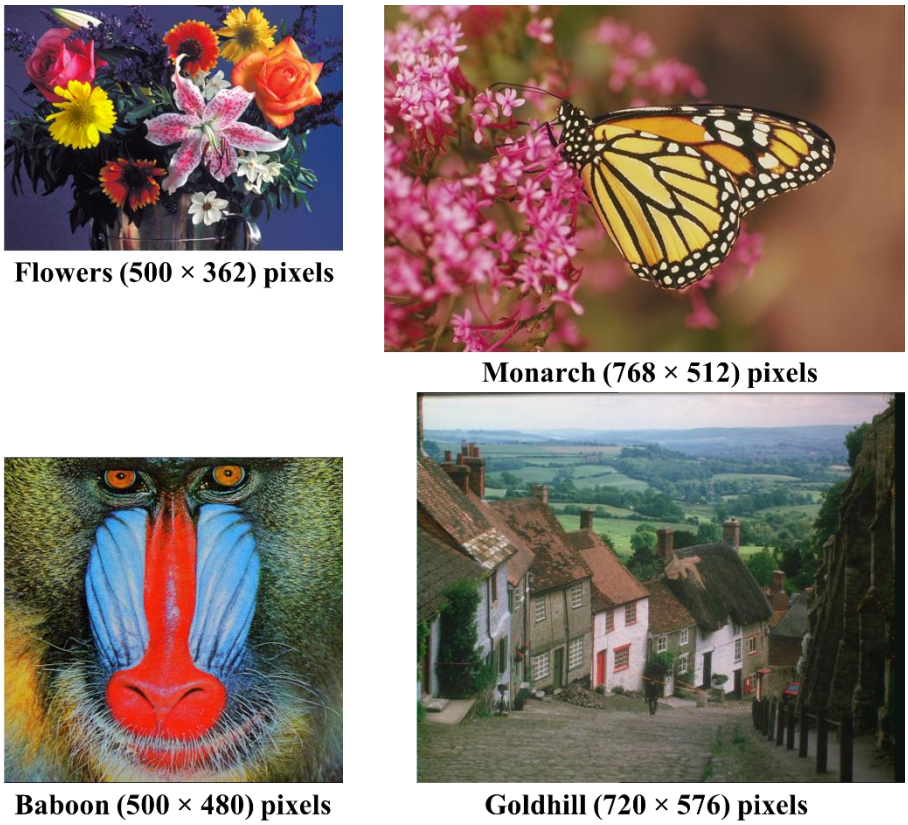

Figure 5. Original image data

The received images are put through grayscale conversion, reducing the dimensionality of the images and making the processing of encryption algorithms simple. Grayscale images are those images that convert color images into shades of gray. In a grayscale image, the value of each pixel shows how bright that pixel is. The formula for transforming images to grayscale is given as[22]:

$$I_{gray}(x, y) = 0.2989R + 0.587G + 0.114B \quad (12)$$

Grayscale transformation of the image is shown in Figure 6. Moreover, if images are not square, pad them to $M \times M$ (where M = max (H , W)) using zero values of pixels. The original dimensions $H \times W$ will be stored using the indexed hash table of the Henon map for decryption.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

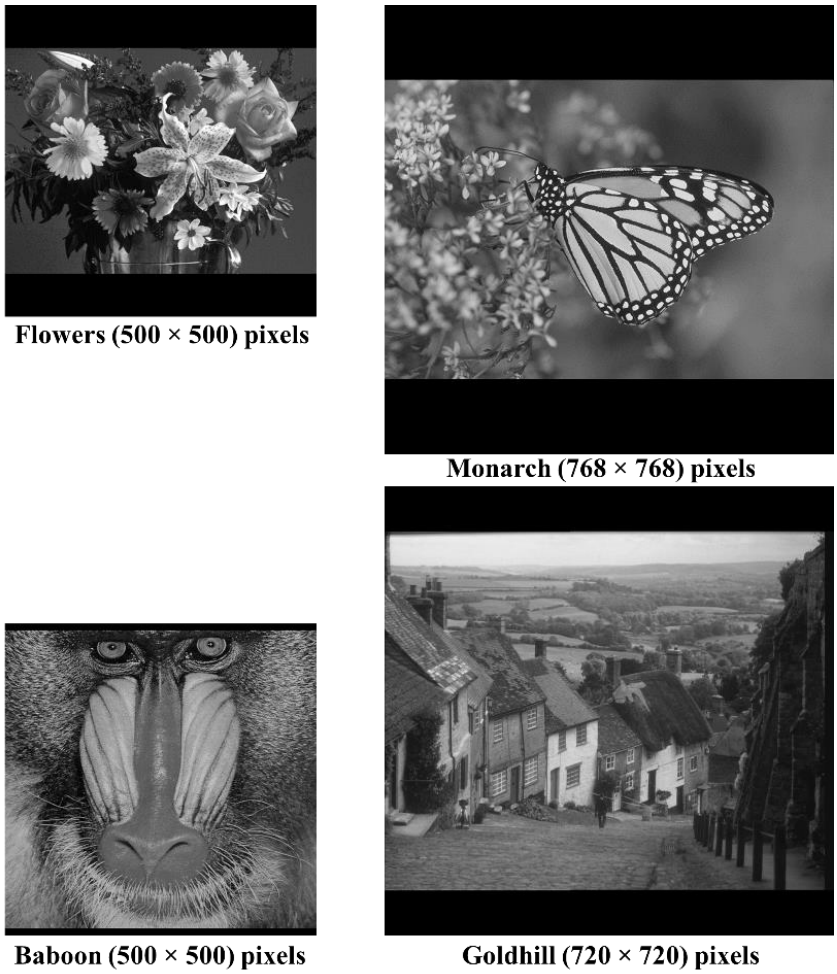

Figure 6. Results of image square and grayscale transformation

B. Proposed Algorithm Overview

The proposed algorithm involves two primary stages: encryption stage and decryption stage. Here is what the encryption stage consists of:

1. Inputting values into the 2D Henon map: is the first step, which is done to put initial values in 2D Henon map to generate chaotic sequences.
2. Using the results of the 2D Henon map as initial values for other chaotic functions: On the output of the Henon map, the algorithm checks two more chaotic functions for further encryption.
3. Image dimension storage using 2D Henon map output as an index: Chaotic sequences that the Henon map outputs are used as indices that will store the dimensions of the image prior to encryption.
4. Use of Arnold map: The map converts the image into grayscale, puts padding to make it a square aspect ratio, and stores original dimensions for later use during decryption.
   The decryption process reverses these steps to retrieve the original image (As shown in Figure 7.). In the next subsections, we provide a detailed explanation of each component of the algorithm.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

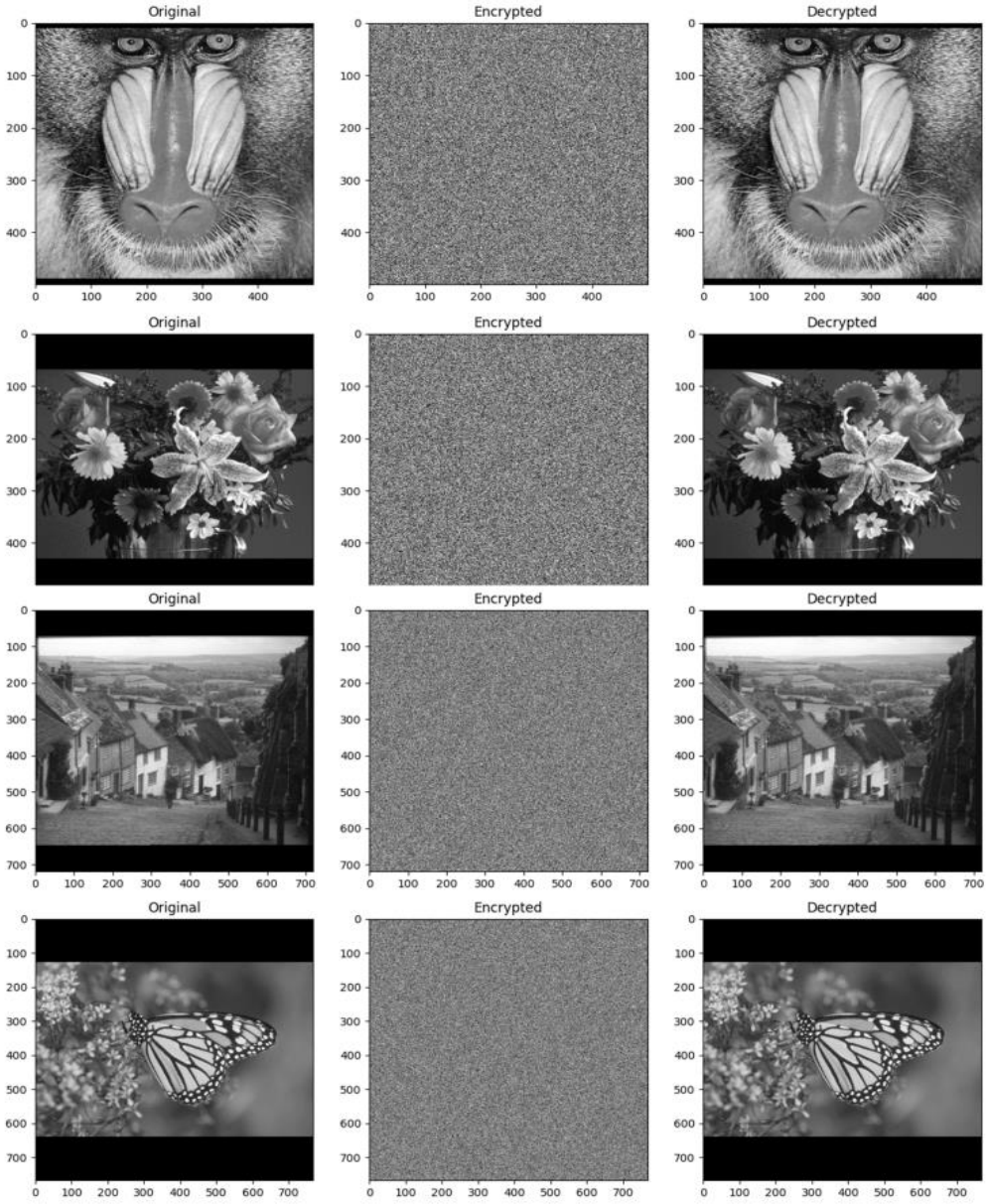

Figure 7. Images before and after encryption process

a. Inputting Values into the 2D Henon Map

The 2D Henon map, a dynamical system operating in discrete time, is characterized by equations 1 and 2. The resulting sequences are then processed to extract binary values (0 or 1) based on predefined thresholds (0.5).

b. Using the Results of the 2D Henon Map as Initial Values for Other Chaotic Functions

The 2D Henon map outputs are used not only for the generation of keys for encryption but they are used as inputs for other chaotic functions as well. Specifically:

1. If output equals 0, the routine applies the memristor element chaotic function for additional encryption.
2. For output of Henon map as 1, the exponential nonlinearity chaotic function is applied for encryption at a next step.

The algorithm enhances the encryption process by adding a layer of complexity and unpredictability. This is achieved through the dynamic selection of one of two distinct chaotic functions, determined by the real-time output generated by the Henon map.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

c. Storing Image Dimensions Using the Results of the 2D Henon Map as Indices

One very important feature of the algorithm is seen in the chaotic sequences that the 2D Henon map will generate and use as indices at which the image dimensions will be stored before encryption. This will guarantee that the original dimensions of the image are safely kept with the encrypted data, on which accurate reconstruction can then take place during decryption.
For example, if the original image has dimensions M×N the algorithm computes a hash like index from the outputs of the Henon map and uses this index to store M and N in a secure way. During decryption, the same outputs of the Henon map are used to retrieve the stored dimensions so that the decrypted image matches the original.

d. Applying the Arnold Map

The following preprocessing steps are applied before applying the Arnold map:
1. Converts the image to grayscale to reduce computational complexity.
2. Resizes the image into a square format by adding padding if necessary. This ensures compatibility with the Arnold map, which requires square matrices.

The Arnold map shuffles the pixel positions in a pseudorandom manner, effectively obfuscating the visual content of the image. The number of iterations of the Arnold map can be adjusted to increase the level of scrambling.

C. Encryption and Decryption Procedures

This section details the proposed methods used to transform images into secure, unreadable formats and the corresponding procedures for restoring them to their original state.

a. Encryption Workflow

1. Chaotic Sequence Generation:
Input initial values into the 2D Henon map to generate chaotic sequences. After that, iterate the Henon map N times to produce $\{(x_i, y_i)\}_{i=1}^{N}, N = M^2$:

$$x_i = 1 - a.x_{i-1}^2 + y_{i-1} - 1, \qquad y_i = b.x_{i-1}$$

2. Conditional Bifurcation:
Use the outputs of the Henon map to select either the memristor element or exponential nonlinearity function for further encryption.

For each $f(x_i) = \begin{cases} r.x_i.(1-x_i) & if\ x_i \le 0.5, \quad (apply\ memristor) \\ \frac{\exp(x_i)}{\exp(1)} & if\ x_i > 0.5, \quad (apply\ exponential) \end{cases}$

Generate: $S_{bifuraction} = \{f(x_i)\}_{i=1}^{N}$

3. S-Box Construction: Generate a 256-length chaotic sequence S_{box} using Henon map, then sort indices:

$$S_{box} = argsort(S_{box})$$

4. Substitution: Pixel values are XORed with S-box:

$$P_{sub}(i) = I_{(i)} \oplus S_{box}[i \ mod\ 256]$$

5. Arnold's Cat Map Permutation:
- Store the original image dimensions using the Henon map outputs as indices.
- Convert the image to grayscale and resize it into a square format.
- Apply the Arnold map to scramble the pixel positions. Shuffle pixel positions using:

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

$$\begin{bmatrix} \acute{x} \\ \acute{y} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ M. \quad (13)$$

The number of iterations is determined by $[1099 \,.\, x_n]$

6. Diffusion: Generate diffusion sequence $D = clip\big(H_{diff}.\,255, 0, 255\big), then$:

$C = (P_{permuted} \oplus \mathrm{D})$ (Element-wise XOR)

b. Decryption Algorithm

Decryption reverses the encryption steps:

1. Retrieve Original Dimensions:

- Extract the chaotic sequences from the ciphertext using the same initial values for the Henon map.
- Use the Henon map's indices to reconstruct $H \times W$.

2. Reverse Diffusion: Reconstruct permuted pixels using the same diffusion sequence: $P_{permuted} = (C \oplus \mathrm{D})$

3. Inverse Arnold's Cat Map: Reverse the Arnold map to restore the original pixel positions. By apply the inverse transformation:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \acute{x} \\ \acute{y} \end{bmatrix} \ mod\ M. \quad (14)$$

Apply for *T* iterations.

4. Reverse Substitution Function: Recover original pixels using the same S-box:

$$\grave{I}_{(i)} = P_{inverse}(i) \oplus S_{box}[i \ \ mod\ 256]$$

5. Remove Padding: Crop the image to $H \times W$. By remove any padding added during resizing and convert the image back to its original format.

5. Results and comparisons

With the increasing reliance on digital images in secure communications, robust encryption techniques are essential to protect sensitive data. However, encrypted images must withstand statistical attacks that exploit patterns to deduce the original content. This section evaluates the statistical resilience of our proposed encryption method.

A. Statistical Attack Analysis

Statistical analysis provides crucial insights into an encryption algorithm's resistance to statistical attacks. Statistical attacks analyze encrypted images for patterns that reveal original content or encryption methods. Effective algorithms produce cipher images devoid of such patterns, which we assess using histograms and correlation coefficients.

a. Histogram Analysis

Histogram analysis is a technique used to evaluate the distribution of pixel intensity values within an image. In the context of secure image encryption, an ideal cipher image should exhibit a uniform histogram, indicating that all pixel intensity values occur with approximately equal frequency. This uniform distribution is crucial for obscuring any statistical patterns that could reveal information about the original image, and it should substantially differ from the original image's histogram. When examining grayscale images (8-bit), all 256 possible intensity values should exist and be uniformly distributed in the encrypted image, even if the original image has a non-uniform distribution[23]. This uniformity prevents attackers from inferring statistical properties of the original image based on frequency analysis. Figure 8. shows the variance of histogram before and after image encryption.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

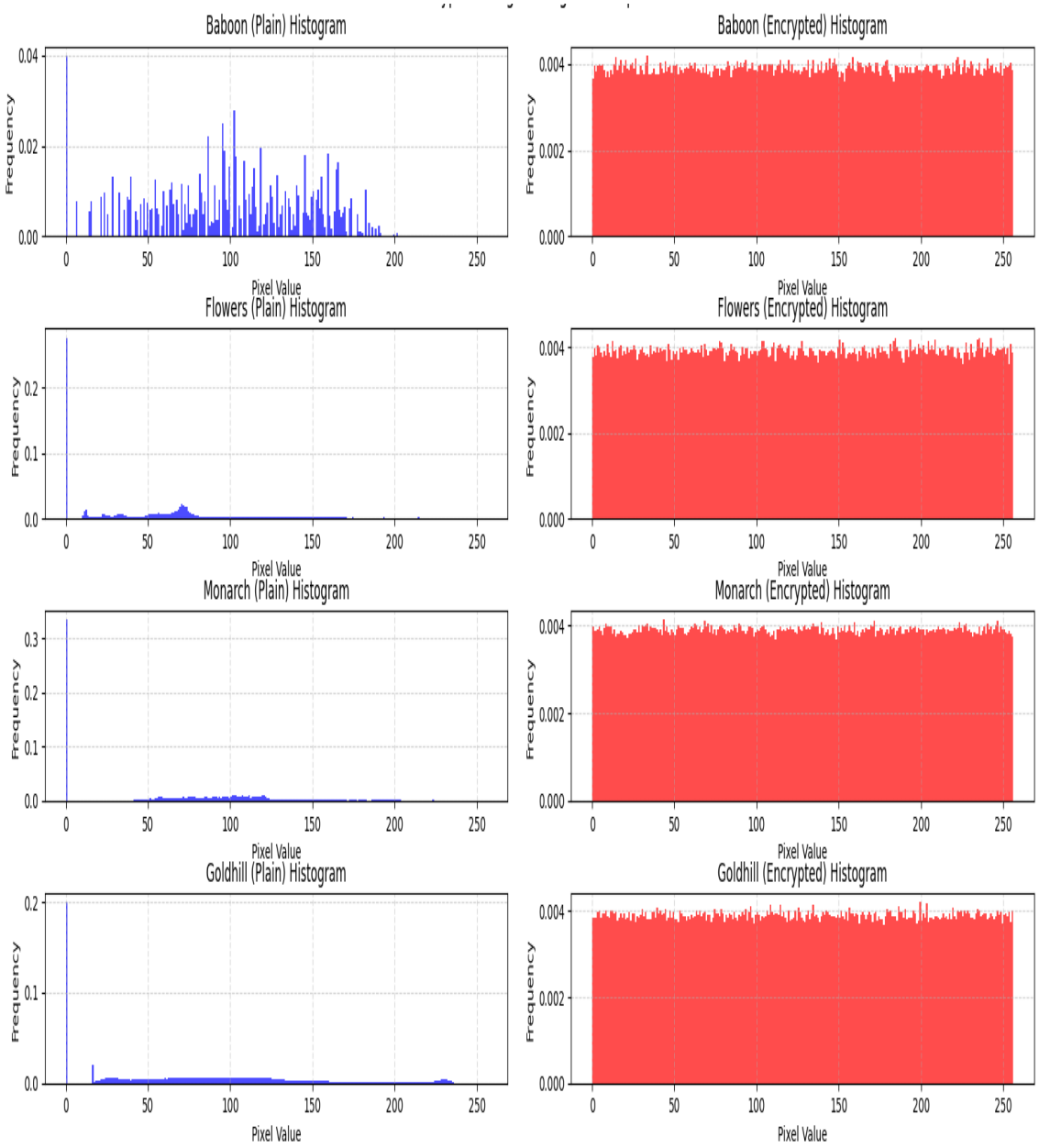

Figure 8. Histogram variance before and after image encryption

The ideal histogram of an encrypted image should demonstrate that pixel values in the range 0-255 are approximately equally distributed, creating a flat histogram profile that differs dramatically from the original image's histogram. This characteristic is particularly important for medical image encryption, where statistical patterns could reveal diagnostic information even in encrypted form[23]. Therefore, the uniform histogram variance before and after encryption in Figure 8. shows that the proposed method effectively obscures image details, enhancing security. This consistency reduces exploitable patterns, making the method robust against attacks. Also, Figure 9 shows the original image, encrypted image and histogram comparison.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

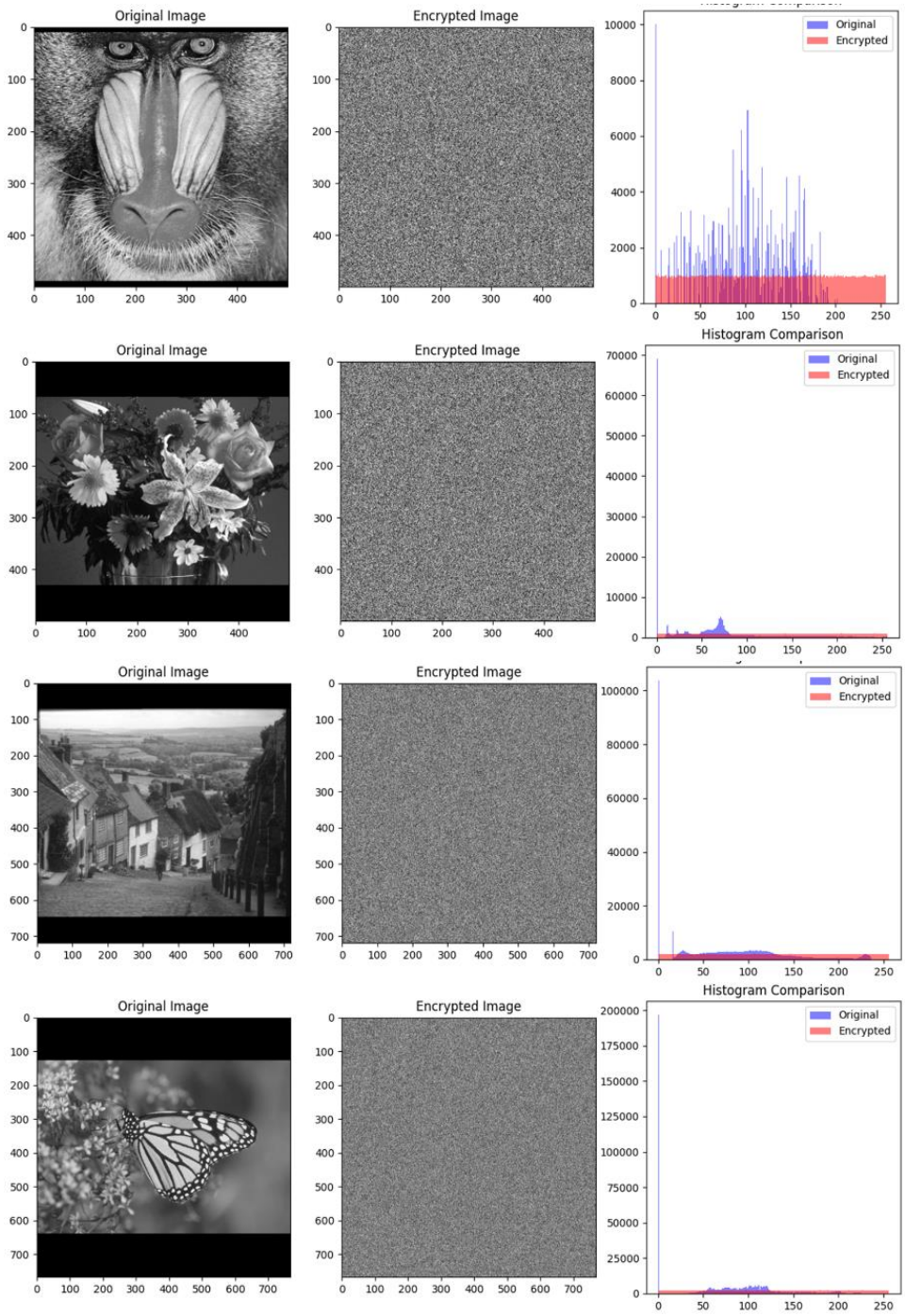

Figure 9. Original image, Encrypted image and Histogram Comparison

b. Correlation Analysis

Correlation analysis evaluates the relationship between adjacent pixels in an image. In natural images, neighboring pixels typically exhibit strong correlation due to the inherent continuity of visual content. An effective encryption algorithm must break this correlation to prevent statistical attacks. Correlation coefficient (CC) quantifies this relationship and is calculated in three directions: horizontal, vertical, and diagonal. The correlation coefficient varies between -1 and +1, with values near zero signifying minimal correlation. For secure encryption, the coefficient for the encrypted image should be close to zero, indicating that adjacent pixels do not share any significant relationship. The formula for calculating correlation coefficient C_{xy} is[13]:

$$C_{xy} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} \quad (15)$$

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

Where $C(x, y)$ represents covariance between coordinates x and y. D(x), D(y) indicate standard deviations. Low correlation values indicate successful disruption of pixel relationships, significantly increasing resistance to statistical attacks.

The correlation coefficient analysis before and after encryption demonstrates the effectiveness of the proposed method in reducing pixel dependency. As shown in the Table 1, the original images have high correlation coefficients (ranging from 0.8484 to 0.9880), indicating strong relationships between adjacent pixels. However, after encryption, the correlation drops significantly to near zero or negative values (ranging from 0.0029 to -0.0177). This drastic reduction confirms that the proposed method effectively eliminates statistical patterns, ensuring that the encrypted image is highly resistant to attacks based on correlation analysis.

Table 1: Adjacent pixel correlation coefficient (CC) for the original and encrypted images

Image	Original image	Encrypted image
Flowers	0.9722	0.0029
Monarch	0.9821	-0.0195
Goldhill	0.9880	-0.0177
Baboon	0.8484	0.0076

B. Quantitative Analysis

To assess the effectiveness and security of the proposed image encryption method, quantitative analyses were conducted using entropy measurements and the Peak Signal-to-Noise Ratio (PSNR). These metrics collectively offer a comprehensive evaluation of both the randomness imparted by the encryption process and the resulting visual distortion.

a. Entropy Analysis

Information entropy quantifies the level of randomness or uncertainty within an image. For an 8-bit grayscale image, the ideal entropy value is 8, representing maximum randomness. A securely encrypted image should exhibit an entropy value approaching this theoretical limit, indicating that its pixel values are highly random and resistant to prediction or analysis. The entropy is calculated using[13]:

$$E(X) = \sum_{j=0}^{255} P_r(X_j) \log_2 P_r(x_j) \quad (16)$$

Where $P_r(x_j)$ is the probability of pixel value x_j. Higher entropy values indicate greater randomness in pixel distribution, making it more difficult for attackers to deduce patterns that could compromise security. The Table 2 clearly demonstrates that the entropy values of the original images are considerably lower, ranging from 5.7077 to 6.7461, indicating the presence of inherent structural patterns and redundancy. In contrast, after encryption, the entropy values for all images consistently approach the theoretical maximum of 8, with values such as 7.99932, 7.99968, 7.99958, and 7.99941 for Flowers, Monarch, Goldhill, and Baboon, respectively. This significant increase in entropy confirms that the proposed encryption method effectively randomizes the pixel distribution, thereby eliminating recognizable patterns and making the images highly resistant to statistical and entropy-based attacks.

Table 2: The information entropy levels of both encrypted and original images

Image	Original image value	Encrypted image value
Flowers	6.1380	7.99932
Monarch	5.7077	7.99968
Goldhill	6.7461	7.99958
Baboon	6.6626	7.99941

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

b. Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) is a standard metric used to evaluate the quality of a reconstructed or compressed image or video by comparing it to the original. Higher PSNR values typically indicate better visual quality and less distortion introduced during processing. It is expressed in decibels (dB) and is commonly used in image processing, compression, and watermarking.
Before computing PSNR, we first calculate the Mean Squared Error (MSE) between the original image I and the distorted (or compressed) image K[24]:

$$MSE = \frac{1}{W \times H} \sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [I(i,j) - K(i,j)]^2 \quad (17)$$

where:
W×H represents the width and height of the image. I(i,j) denotes the pixel value at position (i,j) in the original image, while K(i,j) refers to the corresponding pixel value at the same position in the distorted or encrypted image. Once MSE is computed, PSNR is calculated as:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (18)$$

MAX_I = Maximum possible pixel value (e.g., 255 for 8-bit grayscale images)
The evaluation of the proposed image encryption method shows that the Mean Squared Error (MSE) between the original and decrypted images is zero, leading to a Peak Signal-to-Noise Ratio (PSNR) approaching infinity, which indicates perfect reconstruction without any loss. This outcome indicates a perfect reconstruction of the original image following the decryption process, with no perceptible loss of data or quality. The zero MSE confirms that the encryption and subsequent decryption processes are completely lossless, preserving the integrity of the image content. Meanwhile, an infinite PSNR underscores that there is no degradation in image fidelity, making the proposed method highly suitable for applications requiring exact recovery of the original image data.

C. Differential Attack Analysis

Differential analysis assesses an encryption algorithm's sensitivity to slight modifications in the input image. This evaluation typically relies on two key metrics: the Number of Pixels Change Rate (NPCR), which measures the percentage of differing pixels, and the Unified Average Changing Intensity (UACI), which quantifies the average intensity variation between two ciphered images[13].
NPCR measures the percentage of pixels that change value when a single pixel is modified in the original image, calculated as:

$$NPCR = \frac{\sum_{m,n} D(m,n)}{W \times L} \times 100\%, Where: D(m,n) = \begin{cases} 1, & if\ (E_1(m,n) \neq E_2(m,n) \\ 0, & if (E_1(m,n) = E_2(m,n) \end{cases} \quad (19)$$

Where $D(m,n)$ equals 1 if the corresponding pixels in the two encrypted images differ, and 0 otherwise. For secure encryption, NPCR should exceed 99%.
UACI measures the average intensity difference between the encrypted images, calculated as[23]:

$$UACI = \frac{1}{W \times L} \sum_{mn} \frac{|E_1(m,n) - E(m,n)|}{255} \times 100\% \quad (20)$$

Where E1 and E2 are the two encrypted images. The ideal UACI value for a 512×512 image is approximately 33.46%. These metrics confirm that small changes in the original image produce significantly different encrypted outputs, demonstrating resistance to differential attacks.
As can be seen in Table 3, NPCR values of all test images are between 99.61% and 99.62%. This indicates that almost all pixels change to a large extent when a minor change is applied to the plaintext image. The high NPCR value confirms that the provided encryption technique effectively destroys the relationship between the original and encrypted images and thereby makes it considerably robust against differential attacks. Similarly, the UACI values range from 34.09% to 37.43%, indicating an enormous intensity difference between the original and encrypted images. These results validate that the proposed method ensures strong security by significantly altering pixel values, preventing attackers from deriving meaningful information through differential analysis.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

Table 3: Images evaluated using UACI and NPCR

Image	Dimensions (pixels)	UACI (%)	NPCR (%)
Flowers	500 × 500	37.43	99.62
Monarch	768 × 768	35.61	99.62
Goldhill	720 × 720	34.77	99.62
Baboon	500 × 500	35.08	99.61

D. Key Analysis

The security of an encryption algorithm heavily depends on its key characteristics. Key analysis evaluates aspects such as key space size and sensitivity to minor key modifications.

a. Key Space Analysis

Key space refers to the total number of possible unique keys that an encryption algorithm can utilize. A large key space is essential to prevent brute-force attacks, where attackers systematically check all possible keys. The minimum acceptable key space in modern cryptographic systems is 2^{128}, though larger spaces provide greater security margins[13][25].

The key space of the encryption scheme is derived from multiple chaotic and nonlinear components, each contributing to cryptographic strength. The core parameters of the Henon map (a, b, $x_0, and\ y_0$) are represented as 64-bit double-precision floating-point numbers. Each parameter offers 2^{64} possible values, leading to a base key space of:

$$(2^{64})^4 = 2^{256}$$

The diffusion layer introduces modified initial conditions ($x_0 + 0.1,\ y_0 + 0.1$), which are derived from the core keys but add dependency depth. This effectively doubles the key material, contributing an additional 2^{256}, resulting in:

$$2^{256} \times 2^{256} = 2^{512}$$

Arnold's permutation uses a chaotically derived iteration count $(100 \times Henon_{x[-1]})$, which varies between 100–150 cycles. This adds $\log_2 150 \approx 8\ bits$ (2^8) to the key space. The S-box generation employs a permutation of 256 values via chaotic sorting, contributing $\log_2 256! \approx 1684\ bits$ (2^{1684}). Finally, the chaotic sequences (2× image size) amplify sensitivity to parameter changes, though their length is dynamically determined by the core keys.

Combining all components, the total key space is:

$$2^{256} \times 2^{256} \times 2^8 \times 2^{1684} = 2^{2460} \approx 1.7 \times 10^{740}$$

This astronomically large key space 2^{2460} ensures resistance to brute-force attacks, exceeding even advanced standards like AES-256 2^{256}. The integration of multi-source entropy (Henon, memristor, Arnold's map) and nonlinear enhancements (cubic/exponential terms) further strengthens cryptographic robustness.

b. Key Sensitivity Analysis

The Ciphertext Difference Rate (CDR) measures the percentage of differing pixel values between two ciphertexts generated from minimally altered plaintexts or keys. A high CDR (≈99.6%) indicates strong resistance to differential cryptanalysis. The CDR is defined as[25]:

$$CDR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{L} D(i,j)}{W \times L} \times 100\% \qquad (21)$$

W×L is the width and length of the image, and $D(i,j)$ is binary difference function equals 1 if the corresponding pixels in the two encrypted images differ, and 0 otherwise.

As shown in the Table 4, the proposed method achieves consistently high CDR values, ranging from 99.59% to 99.61% across different test images. These results indicate that nearly all pixel values in the encrypted images undergo significant alterations when even a slight change is introduced in the original image. Such high CDR values confirm that the encryption process ensures strong diffusion properties, making the proposed method highly resistant to differential attacks and ensuring that any small modification in the plaintext leads to a completely

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

different ciphertext. This robustness enhances the security of the encryption scheme by preventing attackers from inferring patterns or relationships between the original and encrypted images.

Table 4: Key Sensitivity CDR for different images

Image	Dimensions (pixels)	CDR Value
Flowers	500 × 500	99.61%
Monarch	768 × 768	99.60%
Goldhill	720 × 720	99.59%
Baboon	500 × 500	99.61%

E. Comparative the results with the other studies

Table 5 presents a comparative analysis of the proposed encryption method against existing approaches in terms of key security metrics, including correlation coefficient, entropy of the encrypted image, key size, NPCR, and UACI. The results indicate that the suggested technique surpasses existing techniques in some key aspects, thereby confirming its strength and efficiency in the area of secure image encryption.

One of the most significant strengths of the proposed method is its exceptionally high key size of 2^{2460}, which far exceeds the key sizes used in other methods, ranging from 2^{239} *to* 2^{792}. A larger key space enhances resistance against brute-force attacks, making the encryption scheme highly secure. Additionally, the proposed method achieves an encrypted image entropy of 7.99941, which is closer to the ideal value of 8 compared to other methods, ensuring a near-perfect uniform pixel distribution and eliminating exploitable statistical patterns.

In terms of resistance to differential attacks, the proposed method maintains a competitive NPCR value of 99.61%, which is comparable to or better than most existing approaches. This indicates that even the slightest change in the plaintext image leads to substantial alterations in the ciphertext, preventing attackers from detecting meaningful correlations. Furthermore, the UACI value of 35.08% demonstrates a higher intensity change in encrypted images compared to most prior methods, highlighting the strong diffusion characteristics of the proposed algorithm.

Another key advantage of the proposed method is its near-zero correlation coefficient (0.0076), which confirms that the encryption process effectively eliminates any linear relationship between adjacent pixels. This is crucial for preventing statistical attacks, as encrypted images with a lower correlation coefficient are significantly more resistant to analysis-based decryption attempts.

Overall, the proposed encryption method demonstrates superior performance by achieving a stronger key size, near-ideal entropy, improved NPCR and UACI values, and a near-zero correlation coefficient. These findings highlight the robustness of the encryption scheme in ensuring high security while maintaining effective diffusion and confusion properties[26]. Such advancements are particularly important for secure image transmission and storage in applications where data confidentiality is paramount.

Table 5: Comparative Analysis of the Proposed Algorithm (Baboon image) with Existing Approaches

Methods	Year	Correlation coefficient	Encrypted image entropy	Key size	NPCR (%)	UACI (%)
Proposed method	**2025**	**0.0076**	**7.99941**	**2^{2460}**	**99.61**	**35.08**
[6]	2025	0.00070	7.9754	2^{256}	99.5453	33.4224
[8]	2024	0.05990	7.9976	2^{792}	99.6100	33.62
[7]	2024	0.00070	7.9969	2^{256}	99.5987	33.3539
[12]	2023	-	7.9965	2^{478}	99.6254	33.0704
[9]	2023	-	7.9993	2^{239}	99.60844	33.4467
[10]	2022	0.01910	7.9993	2^{498}	99.6048	33.4024
[11]	2021	0.01600	7.9993	2^{448}	99.5461	35.9229

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

6. Conclusion

This study presents a hybrid image encryption framework integrating Arnold and Henon map's bifurcation behavior, memristor elements, and exponential nonlinearity chaos. By dynamically selecting chaotic functions and binding keys to image features, the scheme achieves near-perfect statistical randomness, infinite PSNR, and resistance to differential and brute-force attacks. A keyspace of 2^{2460} and 99.61% key sensitivity CDR ensure long-term security. The proposed method resists cryptanalysis while maintaining efficiency. Future work could explore optimizing the algorithm for real-time applications and extending it to video encryption.

References

[1] N. Khurana and M. Dua, "A novel one-dimensional Cosine within Sine chaotic map and novel permutation–diffusion based medical image encryption," Nonlinear Dyn., vol. 113, no. 5, pp. 4839–4859, 2025.

[2] Y. A. A. S. Aldeen and H. M. Abdulhadi, "Data communication for drone-enabled internet of things," Indonesian J. Electr. Eng. Comput. Sci., vol. 22, no. 2, pp. 1216-1222, 2021.

[3] S. A. Jassim, A. K. Farhan, and A. H. Radie, "Using a Hybrid Pseudorandom Number Generator for Cryptography in the Internet of Things," in 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), 2021, pp. 264–269.

[4] S. T. Faraj, S. A. Jassim, and K. K. Kifayat, "Mediated IBC-Based Management System of Identity and Access in Cloud Computing," Tikrit J. Eng. Sci., vol. 20, no. 3, pp. 1–9, 2013.

[5] W. K. Awad, "Searching over encrypted shared data via cloud data storage," Available SSRN 4468120, 2018.

[6] Q. Kadhim and W. A. M. Al-Jawher, "A new multiple-chaos image encryption algorithm based on block compressive sensing, swin transformer, and wild horse optimization," Multidiscip. Sci. J., vol. 7, no. 1, p. 2025012, 2025.

[7] Q. K. Abed and W. A. M. Al-Jawher, "Optimized Color Image Encryption Using Arnold Transform, URUK Chaotic Map and GWO Algorithm," J. Port Sci. Res., vol. 7, no. 3, pp. 219–236, 2024.

[8] Z. Zhuang, Z. Zhuang, and T. Wang, "Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition," Sci. Rep., vol. 14, no. 1, p. 402, 2024.

[9] E. Moya-Albor, A. Romero-Arellano, J. Brieva, and S. L. Gomez-Coronel, "Color image encryption algorithm based on a chaotic model using the modular discrete derivative and Langton's ant," Mathematics, vol. 11, no. 10, p. 2396, 2023.

[10] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "Novel encryption for color images using fractional-order hyperchaotic system," J. Ambient Intell. Humaniz. Comput., vol. 13, no. 2, pp. 973–988, 2022.

[11] I. Ahmad and S. Shin, "A novel hybrid image encryption–compression scheme by combining chaos theory and number theory," Signal Process. Image Commun., vol. 98, p. 116418, 2021.

[12] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," IEEE Access, vol. 11, pp. 11541–11554, 2023.

[13] S. A. Jassim and A. K. Farhan, "Combined Chebyshev and logistic maps to generate pseudorandom number generator for Internet of Things," Int. J. Electr. Comput. Eng., vol. 12, no. 3, 2022.

[14] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," IEEE Trans. Signal Process., vol. 68, pp. 1937–1949, 2020.

[15] H. Nasry, A. A. Abdallah, A. K. Farhan, H. E. Ahmed, and W. I. El Sobky, "Multi chaotic system to generate novel S-box for image encryption," in Journal of Physics: Conference Series, 2022, vol. 2304, no. 1, p. 12007.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025

[16] S. Kvatinsky, E. G. Friedman, A. Kolodny, and U. C. Weiser, "TEAM: Threshold adaptive memristor model," IEEE Trans. Circuits Syst. I Regul. Pap., vol. 60, no. 1, pp. 211–221, 2012.

[17] I. V. Boylo and K. L. Metlov, "Nonlinear effects in memristors with mobile vacancies," R. Soc. Open Sci., vol. 8, no. 10, p. 210677, 2021.

[18] S. Liu, Q. Wang, C. Liu, Y. Sun, and L. He, "Natural Exponential and Three-Dimensional Chaotic System," Adv. Sci., vol. 10, no. 15, p. 2204269, 2023.

[19] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," J. Imaging, vol. 8, no. 6, p. 167, 2022.

[20] H. Liu, B. Zhao, and L. Huang, "Quantum image encryption scheme using Arnold transform and S-box scrambling," Entropy, vol. 21, no. 4, p. 343, 2019.

[21] "Mathship Technologies." [Online]. Available: https://www.hlevkin.com/hlevkin/06testimages.htm. [Accessed: Mar. 29, 2025].

[22] Y. Wu, S. Chu, H. Bao, D. Wang, and J. Zhou, "Optimization of Image Encryption Algorithm Based on Henon Mapping and Arnold Transformation of Chaotic Systems," IEEE Access, 2024.

[23] A. R. Smith and B. J. Johnson, "A Review of Cryptographic Techniques for Secure Image Transmission," J. Inf. Sec. Appl., vol. 58, pp. 102-110, 2022.

[24] L. M. Patel and R. K. Verma, "Performance Analysis of Image Encryption Techniques: A Survey," Int. J. Comput. Appl., vol. 184, no. 9, pp. 29-36, 2021.

[25] T. H. Nguyen and P. A. Tran, "Chaotic Image Encryption Using a Hybrid Approach," J. Cybersecur. Privacy, vol. 1, no. 3, pp. 123-135, 2021.

[26] S. A. Jassim, "Enhancing S-box Generation Using African Buffalo Optimization Algorithm Techniques," Int. J. Intell. Eng. Syst., vol. 18, no. 3, 2025.

DOI: https://doi.org/10.54216/JCIM.160206
Received: December 15, 2024 Revised: February 08, 2025 Accepted: March 02, 2025