STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
*Stat., Optim. Inf. Comput.*, Vol. **15**, May 2026, pp 3998–4020.
Published online in International Academic Press (www.IAPress.org)

# Adaptive Block-Based Color Image Encryption Using Sine and Logistic Chaotic Maps

Fatima KOULOUH [1*], Safae AMINE [1], Mohammed ES-SABRY [2], Nabil EL AKKAD[1]

[1]*LASET, laboratory ENSAF, University of Mohammed Ben Abdellah, Fez, Morocco*
[2]*ISISA, Information Security, Intelligent Systems and Application, Faculty of Sciences, Abdelmalek Essaadi University, Tetouan, Morocco*

**Abstract** This paper presents a robust and reproducible chaos-based encryption scheme for color images by combining the Sine map and a double-stage Logistic map within a block-based framework. Unlike conventional approaches that rely on fixed parameters or unclear key derivation mechanisms, the proposed method dynamically generates chaotic parameters from the statistical properties of the plaintext image, ensuring strong key sensitivity and resistance to cryptanalytic attacks. Initially, the input RGB image is decomposed into three color channels and divided into non-overlapping blocks of size $16\times16$. In the first stage, a Sine map is employed to generate chaotic sequences for each color channel using a control parameter derived from the mean variance of the RGB components. These sequences are generated without direct modification of the image, establishing an initial confusion layer. In the second stage, a Logistic map is used to produce a unique permutation of block indices, enforcing strict uniqueness and enabling a selective XOR diffusion process between image blocks and the previously generated Sine sequences. This operation produces an intermediate encrypted image. To further enhance security, a second diffusion stage is introduced. New Sine map sequences are regenerated using the same chaotic control parameter but with initial conditions dynamically extracted from the intermediate image, ensuring plaintext dependency. A second Logistic map with distinct parameters is then applied to generate a new unique block index vector, followed by an additional XOR operation, yielding the final encrypted image. Comprehensive experimental analyses demonstrate that the proposed scheme achieves near-ideal entropy values, negligible pixel correlation in all directions, and strong resistance to statistical and differential attacks. The decryption process accurately reconstructs the original image when the correct keys are provided, confirming the reversibility and reliability of the method. Owing to its simplicity, high security, and computational efficiency, the proposed encryption framework is well suited for secure image transmission and storage applications.

**Keywords** Color Image Security, Cryptography, Sine Map, Logistic Map, Hybrid Techniques

**DOI:** 10.19139/soic-2310-5070-3046

## 1. Introduction

The security of color images is a primary concern in various areas[1] including the secure transmission of visual information and the protection of sensitive graphic data[2, 3]. Faced with these challenges, numerous methods of image cryptography have been developed to strengthen the confidentiality of visual content[4]. In this paper, we will propose a new approach for enhancing color image security by exploiting the robust properties of Sine maps[5]. Additionally, we integrate one-dimensional chaotic transformations to further strengthen the encryption process. This approach relies on the joint application of 1D chaotic transformations (Sine and Logistic maps) to generate highly secure pseudo-random sequences[6, 7, 8].

Sine maps are mathematical tools that exhibit deterministic chaotic behaviors[9, 10, 11, 12]. Their use in cryptography has shown promise due to their ability to generate robust random sequences, making encryption

*Correspondence to: Fatima KOULOUH (Email: fatima.koulouh@usmba.ac.ma). LASET, laboratory ENSAF, University of Mohammed Ben Abdellah, Fez, Morocco.

ISSN 2310-5070 (online) ISSN 2311-004X (print)

algorithms resistant to attacks[13, 14, 15]. This intrinsic property makes Sine maps suitable for designing encryption techniques that can withstand cryptanalytic attacks[16, 17]. Simultaneously, the dual application of Logistic chaotic maps[18] is an advanced strategy exploiting the chaotic behavior of Logistic maps. The use of multiple instance of these maps in the encryption process boosts the algorithm's complexity, thereby improving its resistance to intrusion attempts[19, 20, 21, 22]. Logistic maps, known for their unpredictable and deterministic nature, provide a solid foundation for encryption methods[23]. The integration of Sine maps and Logistic maps allows to combine the advantages of these two chaotic approaches. By using these two types of transformations together, we can create an encryption system that exploits the chaotic properties to generate a highly secure, pseudo-random sequence[24, 25]. This approach provides enhanced protection of color images against cryptanalytic attacks and intrusion attempts. In this article, we will detail our approach based on the synergistic combination of these two powerful techniques, namely Sine maps and the double application of Logistic maps, in order to optimize the security of color images. We will explore the theoretical aspects of these methods by highlighting their respective advantages[26, 27], and describe in detail how they are integrated into our proposal for increased security. Extensive research conducted on applications of Sine and Logistic maps in cryptography[28, 29]. demonstrate their effectiveness in designing robust encryption schemes. However, the exploration of their combined potential, particularly to improve the security of color images, remains a little-explored field[30]. The main contributions of this work are summarized as follows:

- A block-based color image encryption scheme is proposed, where each RGB channel is processed independently using chaotic maps to reduce inter-channel correlation leakage.
- An adaptive key generation strategy is introduced, in which the control parameter of the Sine map is dynamically adjusted based on the statistical variance of the plaintext image, enhancing plaintext sensitivity.
- A two-stage diffusion mechanism based on a double Logistic map is employed to significantly reinforce diffusion and eliminate residual correlations left by a single chaotic phase.
- A mathematically consistent encryption framework is presented, including explicit formulations of chaotic sequence generation, block-wise XOR operations, and final image reconstruction.
- Extensive experimental evaluations demonstrate that the proposed method achieves high security performance, with near-ideal entropy, negligible pixel correlation, and strong resistance against differential attacks.

In the following sections, we will describe our methodological approach, present the results of our experiments, and discuss the practical and theoretical implications of our method in the context of color image security. This research aims to contribute significantly to the evolution of cryptographic techniques dedicated to the protection of visual information.

## 2. Related work

The security of color images is a dynamic area of research, crucial to ensuring the confidentiality and integrity of visual data in various sectors. To reinforce this security, many researchers have studied the field of image encryption in order to design algorithms adapted to the specificities of multimedia data. Most of these algorithms rely on the use of chaotic maps[31, 32, 33, 34], characterized by their sensitivity to initial conditions, variability of system parameters, non-periodicity, and generation of pseudo-random values. Major contributions in this area include the work of Singh et al.[35] explored a secure communications system based on chaos, using a Logistic map as a key element. In their study, they emphasize the effectiveness of this approach in safeguarding the confidentiality of data exchanged within a communication context. By integrating the chaotic principles of the Logistic maps, the proposed system offers a robust method for securing information transmissions, while preserving the integrity of visual data. Similarly, the research of Goumidi et al.[36] proposed an image encryption method based on modified confusion-diffusion, integrating standard, Logistical and Sine chaotic maps to secure satellite images. Their innovative approach combines different chaotic maps to enhance image encryption security, using adapted confusion-diffusion operations. Zeng et al.[37] presented an approach of an image encryption that is based on the Logistic-Sine compound chaos. Their research highlights the performance of this method to ensure the

confidentiality of images in a distributed context. By combining the characteristics of Logistics maps and Sine, their approach offers an efficient and robust solution for image encryption. More recently, research by Zhou et al.[23] introduced an innovative encoding system that leverages a system of conservative hyperchaotic and diffusion of closed-loop between blocks. Their study shows how this approach provides enhanced security for visual data, using a chaotic system for encryption and inter-block diffusion for data confusion. Kiran et al.[38] proposed partial image encryption which is based on athe Sine Logistics Maps (LSM). Their research highlights the capabilities of this approach to ensure the confidentiality of specific image regions, using the LSM maps as an effective encryption tool. Elazzaby et al.[39] present a significant advancement in image cryptography using the bidimensional Arnold Cat Map to rearrange pixel positions based on parameters from the original image. Introduced with the blur patterns, the multiplicative group Z/nZ, generated from a 2D Logistic-sinusoidal map derived hyper-chaotic sequence, adds random changes to the statistical properties of the encrypted image. By exploiting the properties of multiplicative groups and chaotic systems, they were able to demonstrate a robust and efficient method for encrypting visual data. In[27], image encryption using a 2D sinusoidal Logistic modulation map and the Z/nZ group to create a highly secure encryption method. By exploiting hyper-chaotic properties, it generates a blurred pattern that obscures the original image. Comparative tests show that this approach achieves high security, optimal complexity and strong protection against unauthorised access, Surpassing the existing methods. Es-Sabry et al.[40], presents a highly efficient color image encryption algorithm through Logistic Map, Sine, Chebyshev multiple maps and intersecting plane technique in a cube. The algorithm encrypts each color channel (red, green, blue) by first extracting pixel values and performing circular rotations to ensure uniqueness, followed by encryption using intersecting planes and the Arnold Cat Map for confusion. The method demonstrates high performance, reliability, and robustness compared to existing techniques. Another more recent work by Es-Sabry et al.[41], proposes a method for encrypting 32-bit color according to 4 one-dimensional chaotic maps (Tent, Logistic, Chebyshev, Sine) and 16 $\times$ 16 matrices for each color channel. The process involves shifting pixel values, encrypting them with the Four-square cipher, and using the Arnold Cat Map for pixel rearrangement. Evaluations demonstrate the algorithm's strong performance and security against common attacks. Overall, this research highlights the efficiency and versatility of chaotic maps, including Sine and Logistic maps, in the field of color image security. Their combined use offers promising solutions to strengthen the protection of sensitive visual data, while meeting the performance and efficiency requirements necessary for practical applications.

## 3. Proposed method

In this section, we present the proposed color image encryption algorithm based on a hybrid chaotic framework that combines the Sine map with a double application of the Logistic map. The encryption process starts with the decomposition of the original color image of size $M \times N$ into its three RGB channels, each of which is processed independently and partitioned into non-overlapping blocks of size 16×16. An adaptive control parameter for the Sine map is then automatically derived from the average variance of the 3 color channels, ensuring strong dependence on the plaintext image. Using this parameter, chaotic sequences are generated by the Sine map without modifying the image at this stage. In the subsequent phases, two distinct Logistic maps with different secret keys are employed to generate unique block index permutations. These permutations determine the block positions that are XORed with the corresponding Sine map sequences in two successive encryption stages. The first Logistic map produces an intermediate encrypted image, while the second Logistic map further enhances diffusion and confusion to obtain the final cipher image.

### *3.1. Logistic map*

The Logistic maps, a predominant chaotic mapping function, find extensive application in chaotic crypto systems. Understanding the characteristics and dynamics of the Logistic map is crucial. This maps are extremely sensitive to the initial value. When the parameter $\alpha$ is within the range $[3.57, 4]$, the function exhibits chaotic behavior due to its non-linear nature. The mathematical representation of the Logistic maps is presented in following equation[42]:

$$X_{n+1} = G(\alpha, y_n) = \alpha \times y_n(1 - y_{n+1}) \tag{1}$$

With $\alpha \in [0,4]$ and $y_0 \in [0,1]$. Visually presents the chaotic features of this board. The bifurcation diagram highlights the chaos zone in the interval $[3.57;4]$, an observation supported by the Lyapunov exponent diagram. More specifically, Lyapunov exponent values are negative for $\alpha < 3.57$ and become positive for $\alpha \geq 3.57$. In addition, the values recorded on the diagram are in the range $[0;1]$. To formalize the sequences generated with the Logistic maps for the different channels (red, green and blue) in matrices that match size of original image, the following formula is used:

$$G'(\alpha, y_0) = E(255 \times G(\alpha, y_n)) \tag{2}$$

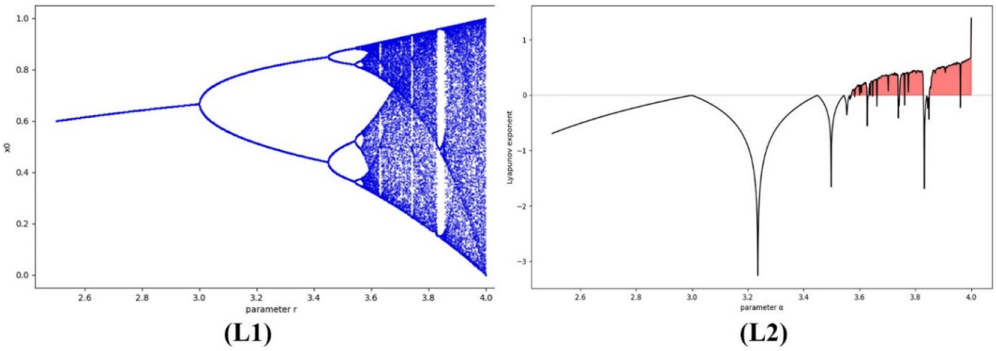



Figure 1. (L1) Bifurcation Diagram of Logistic Map. (L2) Lyapunov exponent Diagram Logistic Map.

### *3.2. Sine map*

Sine map is a method that integrates the Sine function into security algorithms to generate unpredictable elements. This approach exploits the chaotic characteristics of the Sine function to introduce randomness, thus strengthening data protection in cryptographic systems. It is a non-linear function exhibiting a chaotic attitude same to the Logistic maps, and it's defined by[43]:

$$S_{n+1} = T(r, x_n) = r \times x_n \times \sin(\pi \times x_n) \tag{3}$$

With $r \in [0,4]$ and $x_0 \in [0,1]$.

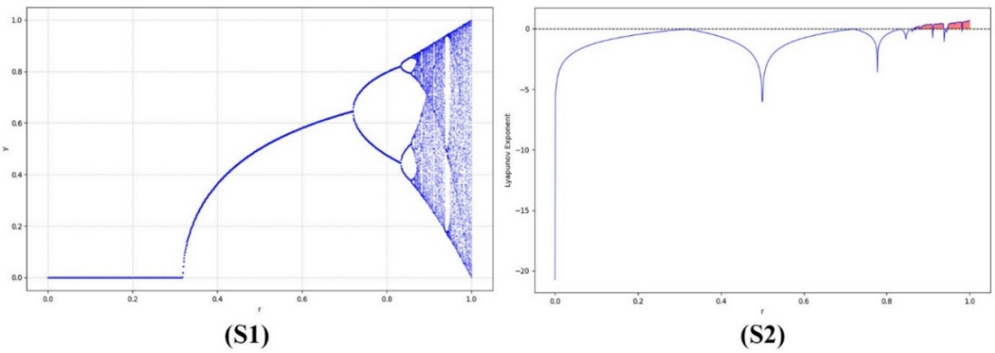



Figure 2. (S1) Bifurcation Diagram of Sine Maps. (S2) Lyapunov exponent Diagram Sine Maps.

### *3.3. Proposed encryption process*

It should be noted that all chaotic parameters and initial conditions are considered secret keys. The chaotic control parameters are carefully selected from ranges known to produce fully chaotic behavior, ensuring high sensitivity and unpredictability. Moreover, the encryption process is fully reversible, allowing accurate image decryption when the correct secret keys are used. Any slight modification in these parameters leads to complete decryption failure, as demonstrated in the key sensitivity analysis.

*3.3.1. Detailed interpretation of the method*

The proposed encryption method is designed as a multi-stage chaotic process that combines confusion and diffusion mechanisms. First, the original color image is decomposed into its red, green, and blue channels. Each channel is processed independently to prevent inter-channel correlation leakage. Chaotic sequences generated by the Sine map are used in the initial diffusion stage, where pixel values are encrypted through bitwise XOR operations. Subsequently, two successive diffusion stages based on Logistic maps are applied, each using independent chaotic parameters. This layered structure enhances sensitivity to secret keys and plaintext variations. The combination of Sine and double Logistic maps ensures strong randomness, high key sensitivity, and effective resistance against statistical and differential attacks.

S1. Image Representation and Block Decomposition

Let the original color image be represented as:

$$I = \{I(i,j,c)\} \in \mathbb{R}^{M\times N\times 3} \tag{4}$$

Where $(i,j)$ denotes the spatial coordinates and $c \in \{R,G,B\}$ represents the color channels. Each color channel $I_c$ is processed independently and divided into non-overlapping square blocks of size $B \times B$, with $B = 16$. The total number of blocks per channel is defined as:

$$N_b = \frac{M \times N}{B^2} \tag{5}$$

This block-based representation enhances spatial diffusion and reduces local pixel correlation.

S2. Variance-Based Adaptive Control Parameter

To tightly link the encryption process to the plaintext image, the control parameter of the Sine map is adaptively computed using a normalized variance index derived from the input image. For each color channel, the variance is calculated as follows:

$$\varphi_c = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_c(i,j) - \mu_c)^2 \tag{6}$$

where $\mu_c$ denote the mean value of channel $c \in \{R,G,B\}$. The average variance is then defined as:

$$\varphi = \frac{1}{3}(\varphi_R + \varphi_G + \varphi_B) \tag{7}$$

A normalized variance index is computed as:

$$\eta = \frac{\varphi}{255^2} \tag{8}$$

where $\eta \in (0,1)$. The adaptive control parameter of the Sine map is obtained by:

$$R = 3.94 + 0.1 \times \eta \tag{9}$$

where $R \in \{3.94, 4\}$. This formulation ensures that the Sine map operates strictly in its chaotic region and introduces strong plaintext sensitivity.

S3. Phase I: Chaotic Sequence Generation Using the Sine Map The Sine map is defined as:

$$x_{n+1} = R\sin(\pi x_n) \tag{10}$$

where $x_0 \in (0,1)$ is the initial condition. Using the adaptive parameter $R$, a chaotic sequence is generated for each color channel with a total length of $N_b \times B^2$. The sequence is then reshaped into block-sized matrices:

$$S^{(1)} = \{S_1^{(1)}, S_2^{(1)}, \ldots, S_{N_b}^{(1)}\}, S_k^{(1)} \in \mathbb{R}^{B\times B} \tag{11}$$

At this stage, the generated sequences are not yet applied to the image and serve as key-dependent masks for the next phase.

S4. Phase II: Block Permutation and Confusion Using Logistic Map 1 The Logistic map is expressed as:

$$y_{n+1} = \alpha_1 y_n(1 - y_n) \tag{12}$$

where $y_0 \in (0,1)$ and $\alpha_1 \in (3.57,4)$ are secret keys. By iterating the Logistic map $N_b$ times, a chaotic sequence is obtained and sorted to generate a unique permutation vector:

$$\Pi^{(1)} = \{\pi_1^{(1)}, \pi_2^{(1)}, \ldots, \pi_{N_b}^{(1)}\}, \pi_k^{(1)} \in \{1, \ldots, N_b\} \tag{13}$$

Each block selected by $\Pi^{(1)}$ is XORed with the corresponding Sine map sequence:

$$B_k^{(2)} = B_{\pi_k^{(1)}} \oplus S_k^{(1)} \tag{14}$$

The resulting blocks form an intermediate encrypted image $I^{(2)}$.

S5. Phase III: Dynamic Sine Map Reinitialization To further enhance diffusion, a new initial condition for the Sine map is extracted from the intermediate encrypted image:

$$x_0^{(2)} = \frac{\text{mean}(I^{(2)}) \bmod 256}{255} \tag{15}$$

Using the same adaptive control parameter $R$, a new chaotic sequence is generated:

$$S^{(2)} = \{S_1^{(2)}, S_2^{(2)}, \ldots, S_{N_b}^{(2)}\} \tag{16}$$

This mechanism ensures strong interdependence between encryption stages.

S6. Phase IV: Final Block Confusion Using Logistic Map 2 A second Logistic map with distinct parameters is defined as:

$$z_{n+1} = \alpha_2 z_n (1 - z_n) \tag{17}$$

where $z_0 \in (0,1)$ and $\alpha_2 \in (3.57,4)$. After generating a second unique permutation vector:

$$\Pi^{(2)} = \{\pi_1^{(2)}, \pi_2^{(2)}, \ldots, \pi_{N_b}^{(2)}\} \tag{18}$$

the final encrypted blocks are obtained by:

$$B_k^{(3)} = B_{\pi_k^{(2)}}^{(2)} \oplus S_k^{(2)} \tag{19}$$

The encrypted image for each color channel is reconstructed by placing the encrypted blocks back into their original spatial order. This operation can be expressed as:

$$E_c = \bigcup_{k=1}^{N_b} B_k^{(3)}, c \in \{R, G, B\} \tag{20}$$

where $\bigcup$ represents the block concatenation operation according to the original block layout. Finally, the encrypted color image is obtained by combining the three encrypted channels:

$$E = \{E_R, E_G, E_B\} \tag{21}$$

**Algorithm 1: Proposed Color Image Encryption Scheme**

→ **Inputs:** Original color image $I$ of size $M \times N \times 3$, secret keys $(x_0, x_0', y_0, z_0, \alpha_1, \alpha_2)$.

→ **Output:** Final encrypted image $E$.

1. **Preprocessing and Decomposition**

– Decompose the image into RGB channels: $I^c$, where $c \in \{R, G, B\}$.

– Divide each channel into non-overlapping blocks $B_k^{(1)}$ of size $16 \times 16$.

– Compute the total number of blocks: $N_b = \dfrac{M \times N}{B^2}$.

2. **Adaptive Parameter Computation**

– Compute the mean variance $\bar{\varphi}$ of the three channels using Eqs. (6) and (7).

– Compute the normalized variance index: $\eta = \dfrac{\bar{\varphi}}{255^2}$.

– Derive the adaptive sine control parameter: $R = 3.94 + 0.1 \times \eta$.

3. **Encryption Phase I (Confusion and Diffusion)**
   - Generate the chaotic sequence $S^{(1)}$ using the sine map: $x_{n+1} = R\sin(\pi x_n)$.
   - Generate the permutation vector $\Pi^{(1)}$ using Logistic map 1: $y_{n+1} = \alpha_1 y_n(1-y_n)$.
   - For each block $k = 1$ to $N_b$, compute: $B_k^{(2)} = B_{\Pi_k^{(1)}}^{(1)} \oplus S_k^{(1)}$ (block permutation and XOR operation).
4. **Encryption Phase II (Dynamic Reinitialization)**
   - Extract the new initial condition: $x_0^{(2)} = \dfrac{\text{mean}(I^{(2)}) \bmod 256}{255}$.
   - Regenerate the chaotic sequence $S^{(2)}$ using the sine map with parameters $R$ and $x_0^{(2)}$.
   - Generate the permutation vector $\Pi^{(2)}$ using Logistic map 2: $z_{n+1} = \alpha_2 z_n(1-z_n)$.
   - For each block $k = 1$ to $N_b$, compute: $B_k^{(3)} = B_{\Pi_k^{(2)}}^{(2)} \oplus S_k^{(2)}$.
5. **Reconstruction**
   - Concatenate the encrypted blocks $B_k^{(3)}$ for each channel: $E^c = \bigcup_{k=1}^{N_b} B_k^{(3)}$.
   - Merge the three channels to obtain the final encrypted color image: $E = \{E^R, E^G, E^B\}$.

Following this analysis, we propose an explanation of the proposed workflow procedure, illustrated by a diagram. This graphic representation, designed as a didactic tool, facilitates the understanding of the encryption procedure. The visual format, known for its pedagogical effectiveness, improves the clarity and accessibility of the proposed cryptographic method, as shown in Figure 3.

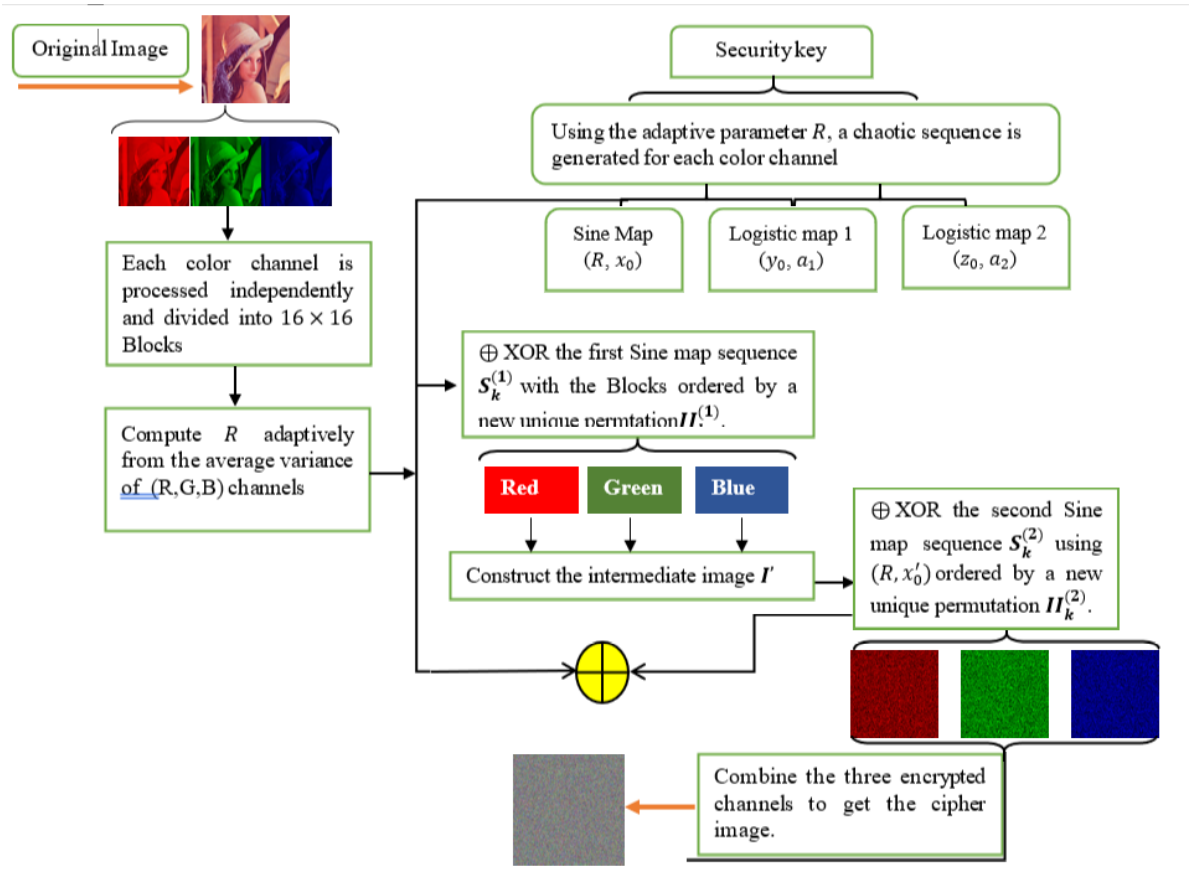



Figure 3. Flowchart of the proposed method

## 4. Experimental results

### *4.1. Statistical analysis*

The intention of this section is to present a comprehensive examination of the postulated primitive cryptography's security and efficiency against reported hacking methods from the literature. The attacks include a statistical analysis where statistical techniques are used on the cryptographic data. This involves studying features or characteristics of the encrypted or decrypted data in an attempt to extract information or ascertain weaknesses. To do this, we applied five various forms of security on images and the operation was performed using the Python programming language.

#### *4.1.1. Execution Time Analysis*

Execution time in-depth analysis was performed for a variety of image sizes, in order to dispel any doubts about the computational cost of the proposed hybrid cryptographic method. The main points that will be discussed in this section are performance according to the algorithm's execution time and its comparison to similar cryptographic methods.

**Experimental Setup**

- Processor: Intel(R) Core (TM) i5-4300U CPU @ 1.90GHz 2.49 GHz.
- Programming Environment: Python 3.9, with libraries including NumPy and Pillow for optimized calculations.
- RAM: 8GB
- Dataset: A dataset consisting of multiple-sized 32-bit color images was used. The encryption technique put forward was applied to every image in sequence, with execution times measured by Python's time module. Each operation was independently timed and repeated across scenarios for consistency and measurement of true performance metrics.

Table 1. The measured execution times for the algorithm on different image sizes

| Image size | Execution Time(seconds) |
|---|---|
| $180 \times 180$ | 0.066959 |
| $256 \times 256$ | 0.100702 |
| $450 \times 450$ | 0.348799 |
| $512 \times 512$ | 0.4453705 |
| $1024 \times 1024$ | 1.747998 |

The results are summarized in Table 1 It can be seen that the execution time is roughly proportional to the number of pixels in the image. For medium-sized images ($512 \times 512$), execution time is as low as 0.445 seconds, which proves the suitability of the method for applications that give priority to security over real-time constraints. For larger images ($1024 \times 1024$), the execution time remains reasonable at 1.747 seconds.

Table 2. A comparison to other approaches in terms of execution time (seconds)

| Method | Execution Time | CPU | RAM |
|---|---|---|---|
| Proposed Hybrid Method | 0.44537 | 2.49 GHz | 8.00 G |
| F. Elazzaby et al.[31] | 1.56623 | 2.50 GHz | 4.00 G |
| M. El-Hajj et al.[44] | 1.76970 | 2.30 GHz | 4.00 G |
| X. Chai et al.[45] | 3.9593 | 3.30 GHz | 4.00 G |
| K. Xuejing et al.[46] | 9.0016 | 2.7 GHz | 8.00 G |

Table 2 compares the suggested scheme's execution time to alternative techniques for encrypting $512 \times 512$ pixel color images. Even under different testing conditions, our proposed algorithm performs better than others, which are optimized under similar conditions. The findings obtained show that the encryption process may be completed at remarkable speeds using the method we have provided, making it ideal for real-time applications.

### *4.1.2. Histogram*

To measure the intensity of distribution in digital and original images, the histogram is generally used as the most familiar measure for representing the distribution[47, 48]. In light of the above, we applied the comparative analysis histogram from eight different original images each containing a different content to their digital equivalent of our counterparts using our innovative method. Looking at the details of the study and referring to the figures 4, 5, 6, 7 and 8 , they found that the histogram, expressed in terms of pixels of the encrypted images, resembles a uniform assignment. However, when comparing the original pictures histograms, there was a big difference in one image while the other had much higher values in a different region. These significant differences between the two histograms will support our argument that our algorithm provides security and prevents images from statistical attacks.

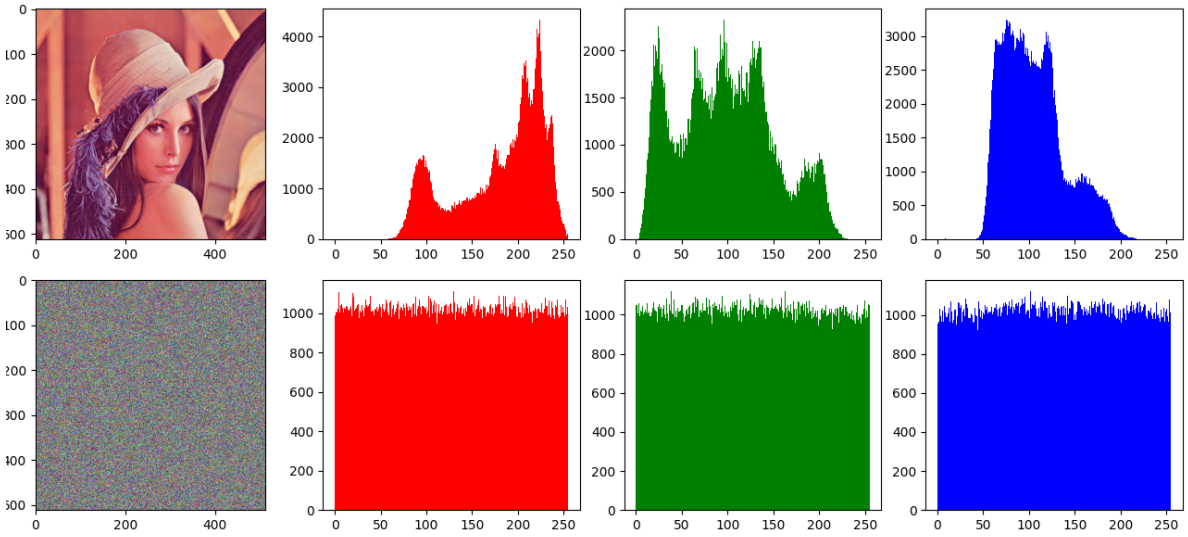


Figure 4. Histograms of the encoded and original Lena images

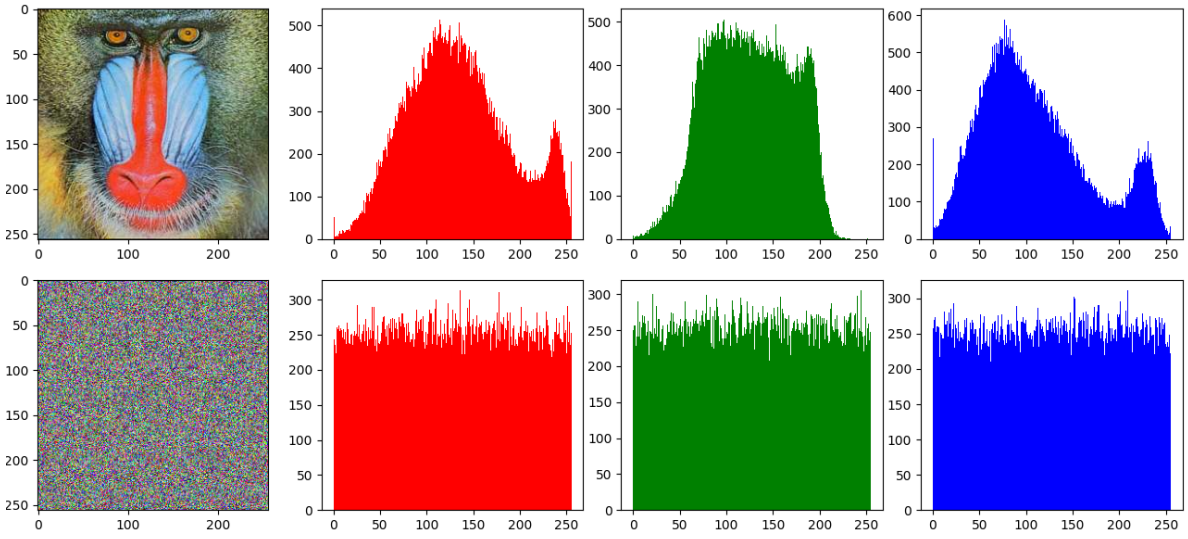


Figure 5. Histograms of the encoded and original Baboon images

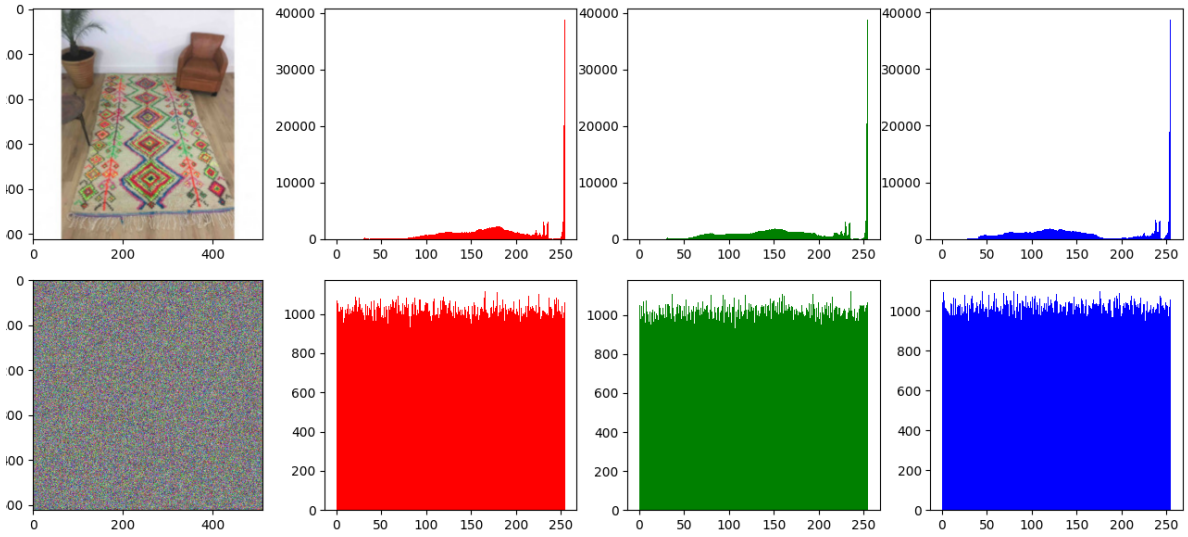


Figure 6. Histograms of the encoded and original Tapi images

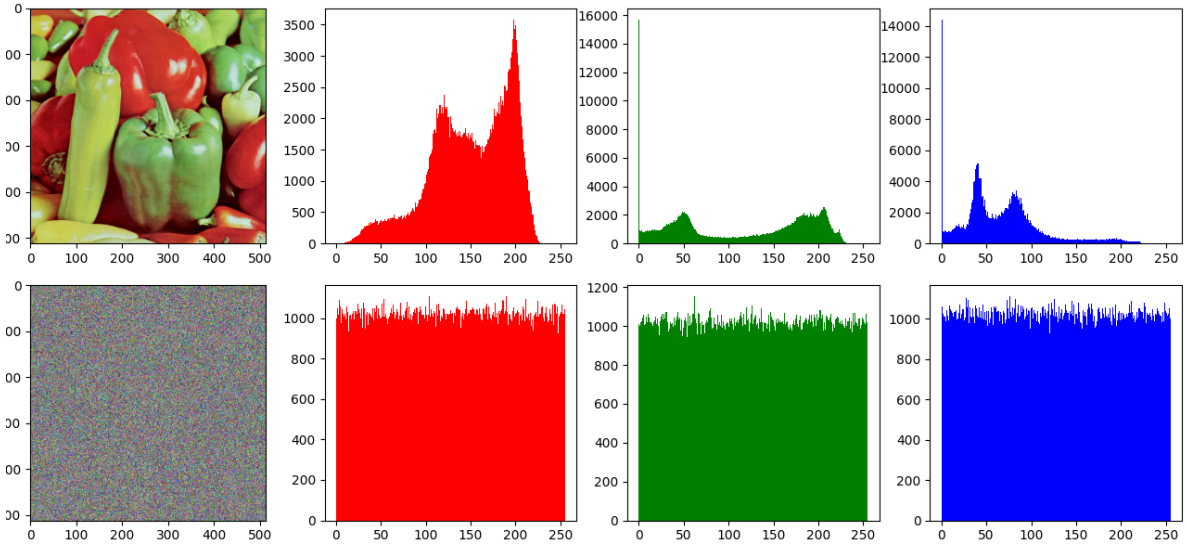


Figure 7. Histograms of the encoded and original Peppers images

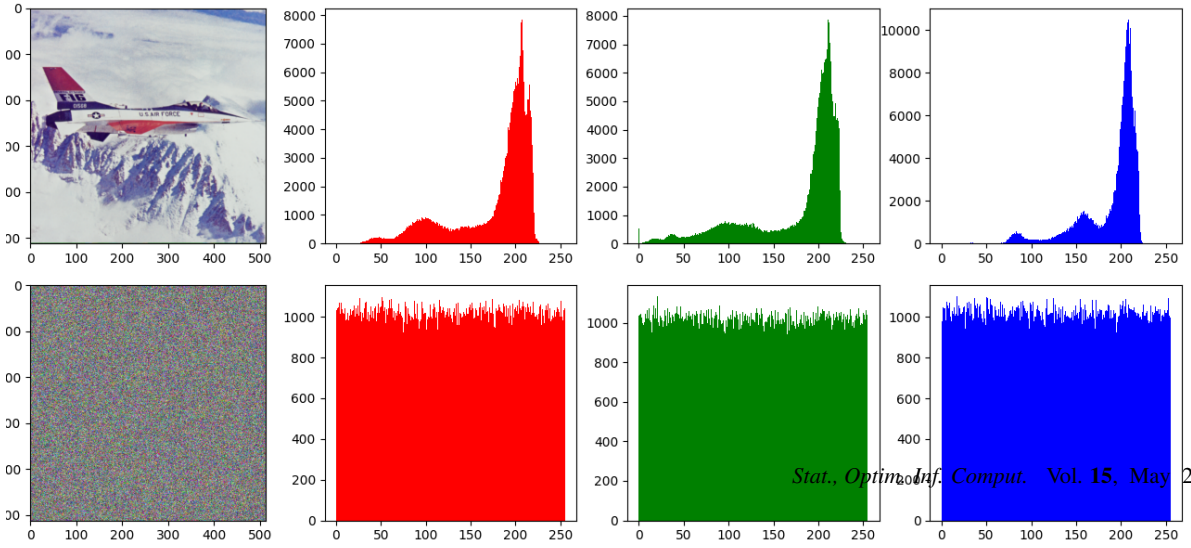


Figure 8. Histograms of the encoded and original Airplane images

*4.1.3. Correlation analysis between neighboring pixels*

Clear images show significant correlations between all adjacent pixels. An effective image encryption system must eliminate this correlation to ensure adequate protection against statistical analysis. To evaluate the potency of our method, a random sample of 30,000 pixels was selected of the clear image and their counterparts in the encrypted image. Subsequently, we computed the correlation coefficients in diagonal vertical and horizontal directions by applying the formula[49, 50]:

$$\mathrm{Cor}_{xy} = \frac{\mathrm{Cov}(x,y)}{\sqrt{L_x}\sqrt{L_y}} \tag{22}$$

$$\mathrm{Cov}(x,y) = \frac{1}{M}\sum_{i}^{M}(x_i - S_x)(y_i - S_y) \tag{23}$$

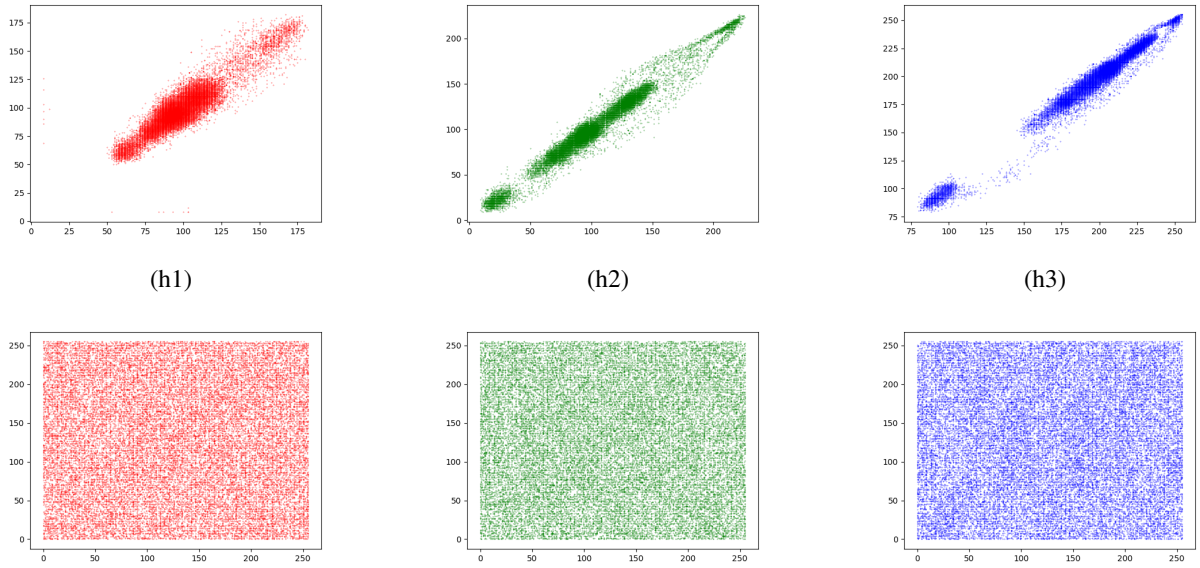
$$L_x = \frac{1}{M}\sum_{i}^{M}(x_i - S_x)^2 \tag{24}$$

$$S_x = \frac{1}{M}\sum_{i}^{M} x_i \tag{25}$$

Table 3. Coefficient of correlation between neighboring pixels in the original and encrypted pictures

| Image | Channels | Original image | | | Encrypted image | | |
|---|---|---|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Lena | R | 0.9889 | 0.9912 | 0.9832 | -0.0045 | 0.0008 | 0.0022 |
| | G | 0.9824 | 0.9840 | 0.9791 | -0.0048 | -0.0012 | -0.0044 |
| | B | 0.9066 | 0.9164 | 0.8927 | 0.0062 | 0.0021 | 0.0046 |
| | Avg | 0.9593 | 0.9639 | 0.9516 | -0.0010 | 0.0005 | 0.0006 |
| Peppers | R | 0.9079 | 0.9323 | 0.8532 | -0.0025 | 0.0064 | 0.0020 |
| | G | 0.9521 | 0.9676 | 0.9227 | 0.0014 | 0.0033 | 0.0030 |
| | B | 0.9018 | 0.9288 | 0.8448 | -0.0025 | -0.0019 | 0.0039 |
| | Avg | 0.9206 | 0.9429 | 0.8736 | 0.0026 | -0.0026 | 0.0029 |
| Tapi | R | 0.8900 | 0.8800 | 0.7845 | 0.0050 | 0.0070 | -0.0051 |
| | G | 0.9100 | 0.9077 | 0.8253 | -0.0021 | 0.0030 | 0.0068 |
| | B | 0.9163 | 0.9207 | 0.8400 | -0.0021 | -0.0042 | -0.0036 |
| | Avg | 0.9054 | 0.9028 | 0.8166 | 0.0024 | 0.0045 | -0.0019 |

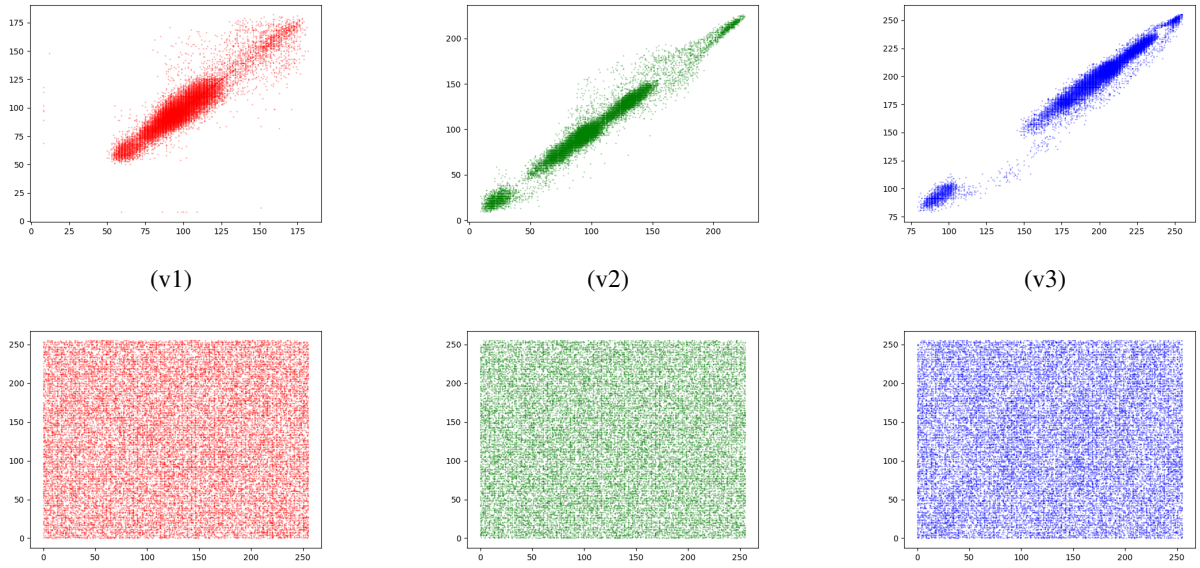
Table 3 represents the calculated values of the correlation coefficient. It is obvious that the correlation coefficients display values close to 1, indicates that these pixels are strongly correlated with those of original images. Conversely, the encrypted image has a correlation coefficient that is approaching to 0, suggesting the absence of correlation between pixels.



(h1) (h2) (h3)

(h4) (h5) (h6)

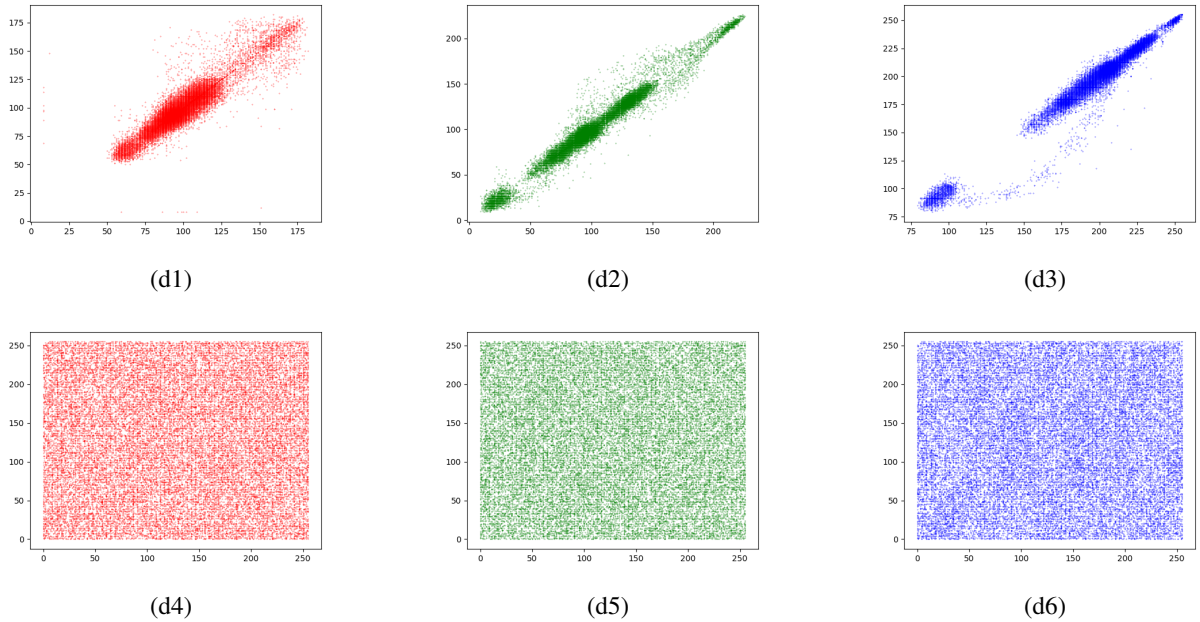
Figure 9. Horizontal correlation distributions of Lena: (h1) original image's red channel; (h2) original image's green channel; (h3) original image's blue channel; (h4) encrypted image's red channel; (h5) encrypted image's green channel; and (h6) encrypted image's blue channel



(v1) (v2) (v3)

(v4) (v5) (v6)

Figure 10. Vertical correlation distributions of Lena: (v1) original image's red channel; (v2) original image's green channel; (v3) original image's blue channel; (v4) original image's red channel; (v5) encrypted image's green channel; and (v6) encrypted image's blue channel



(d1) (d2) (d3)

(d4) (d5) (d6)

Figure 11. Diagonal correlation distributions of Lena: (d1) original image's red channel; (d2) original image's green channel; (d3) original image's blue channel; (d4) original image's red channel; (d5) encrypted image's green channel; and (6) encrypted image's blue channel.

We therefore conclude that, as shown in Figure 9, Figure 10, and Figure 11 our methodology is particularly Mastery of the dependence split between neighboring pixels.

Table 4. The Correlation Coefficient Comparison of adjacent pixels with Other Methods

| Methods | Horizontal | Vertical | Diagonal | Average |
|---|---|---|---|---|
| Folifack Signing VR et al.[51] | -0.0031 | 0.0097 | 0.0005 | 0.00236 |
| Es-Sabry et al.[13] | -0.0072 | 0.0258 | -0.0098 | 0.00294 |
| Benssalah M et al.[52] | 0.0001 | 0.0005 | 0.0015 | 0.00075 |
| Shyamalendu Kandar et al.[53] | 0.0009 | 0.0008 | 0.0027 | 0.00151 |
| Proposed method | -0.0010 | 0.0005 | 0.0006 | 0.00006 |

Table 4 presents a comparison of correlation coefficients between the established methods and the proposed new approach. The results reveal that in some cases my method surpasses the lowest coefficients, which highlights its superior performance. Conversely, there are cases where higher values are observed. Overall, the proposed method demonstrates a very satisfactory level of safety performance.

*4.1.4. Examine the correlation coefficients between the encrypted and original images*

The value of the correlation between each pixel in the source image and the image that needs to be encoded is the primary focus of this analysis. The following formulas will be used in this computation:

$$\mathrm{CC} = \frac{\sum_{i,j}^{M,N}(C_{i,j} - \bar{C})(C'_{i,j} - \bar{C}')}{\sqrt{\sum_{i,j}^{M,N}(C_{i,j} - \bar{C})^2}\sqrt{\sum_{i,j}^{M,N}(C'_{i,j} - \bar{C}')^2}} \tag{26}$$

With

$$\bar{C} = \frac{1}{M \times N}\sum_{i,j}^{M,N} C_{i,j} \tag{27}$$

$$\bar{C}' = \frac{1}{M \times N} \sum_{i,j}^{M,N} C'_{i,j} \tag{28}$$

$C$ is the simple image and $\bar{C}$ is its meaning. Similarly, $C'$ is the encrypted image, and $\bar{C}'$ is its meaning. The dimensions of the matrices $C$ and $C'$ are denoted by $N$ is the length and $M$ is the width, respectively.

Table 5. Comparing the correlation coefficient between the encrypted image and the original image using different techniques.

| Image | Channels | Our Method | El Azzaby et al.[39] | Faragallah et al.[54] | Laiba Asghar et al.[55] | Es-sabry et al.[41] |
|---|---|---|---|---|---|---|
| Lena | R | -0.001070 | - | - | - | 0.00043 |
| | G | -0.000859 | - | - | - | 0.00049 |
| | B | -0.001114 | - | - | - | -0.0025 |
| | Avg | -0.000101 | 0.000486 | 0.020444 | -0.0040 | 0.00055 |
| Baboon | R | -0.003239 | 0.002090 | - | - | - |
| | G | -0.005510 | -0.003772 | - | - | - |
| | B | -0.002017 | 0.002064 | - | - | - |
| | Avg | -0.003588 | 0.000127 | - | - | - |
| Bird | R | 0.001645 | - | - | - | -0.000694 |
| | G | -0.000637 | - | - | - | -0.001227 |
| | B | -0.000751 | - | - | - | -0.002026 |
| | Avg | -0.000085 | - | - | - | -0.001316 |

Table 5 demonstrates that our methodology performs exceptionally in comparison to the outcomes derived from the methodologies outlined in[39], which introduce an innovative image encryption algorithm using multiple chaotic maps with the intersection plane method. Moreover, our approach goes beyond the technique described in[41], which depends on the coupling of a multiplicative group and the chaos theory in the image ciphers, as well as the method explained in[54] And[55]. The value obtained is responsible for this superiority, which shows a remarkable proximity to 0.

### *4.2. Differential attacks*

The proposed cryptographic system demonstrates strong resistance to differential attacks, which aim to exploit small changes in the plaintext image to reveal information about the secret key[49]. An effective image encryption scheme, whether symmetric or asymmetric, must exhibit high sensitivity to minor variations in the original image, such that even a single-pixel modification leads to significant and unpredictable changes in the corresponding ciphertext. To quantitatively evaluate this property, two well-established metrics are employed: the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI). In this study, standard benchmark images including Lena, Baboon, and Bird were used. A slight modification was introduced by altering a single pixel in the plaintext image, and the corresponding encrypted images were generated. The NPCR and UACI values were then computed using Equations (29) and (30), respectively. As reported in Table 6 and Table 7, the obtained NPCR and UACI values for all color channels exceed the critical thresholds defined by Wu et al.[56] at a significance level of $\alpha = 0.05$, namely NPCR = 99.609% and UACI = 33.463%. These results confirm that the proposed encryption scheme provides effective diffusion and strong resistance against differential attacks. Furthermore, the comparative analysis indicates that the proposed method achieves competitive or superior NPCR and UACI performance when compared with several recent chaos-based encryption techniques, highlighting its robustness and reliability.

Table 6. The result of the algorithm's sensitivity to a single pixel change in the original image

| | | Our Method | | El Azzaby et al.[39] | | J. Arif et al.[57] | | Zhou et al.[23] | | Es-sabry et al.[40] | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Image | Channels | NPCR | UACI | NPCR | UACI | NPCR | UACI | NPCR | UACI | NPCR | UACI |
| Lena | Red | 99.66 | 33.87 | 99.77 | 33.48 | - | - | - | - | 99.69 | 33.49 |
| | Green | 99.64 | 33.70 | 99.80 | 33.69 | - | - | - | - | 99.62 | 33.49 |
| | Blue | 99.65 | 33.58 | 99.72 | 33.65 | - | - | - | - | 99.62 | 33.46 |
| | Average | 99.65 | 33.71 | 99.76 | 33.60 | 99.61 | 33.48 | 99.61 | 33.45 | 99.65 | 33.48 |
| Bird | Red | 99.63 | 33.50 | - | - | - | - | - | - | 99.61 | 33.49 |
| | Green | 99.61 | 33.42 | - | - | - | - | - | - | 99.69 | 33.41 |
| | Blue | 99.62 | 33.45 | - | - | - | - | - | - | 99.63 | 33.42 |
| | Average | 99.62 | 33.46 | - | - | - | - | - | - | 99.64 | 33.44 |
| Baboon | Red | 99.57 | 33.48 | - | - | - | - | - | - | - | - |
| | Green | 99.64 | 33.59 | - | - | - | - | - | - | - | - |
| | Blue | 99.62 | 33.52 | - | - | - | - | - | - | - | - |
| | Average | 99.61 | 33.45 | - | - | 99.60 | 33.43 | 99.60 | 33.40 | - | - |

Table 7. Result for NPCR and UACI of the suggested method

| Image | Channels | NPCR(%) | UACI(%) |
|---|---|---|---|
| Lena | Red | 99.66 | 33.87 |
| | Green | 99.64 | 33.70 |
| | Blue | 99.65 | 33.58 |
| | Average | 99.65 | 33.71 |
| Bird | Red | 99.63 | 33.50 |
| | Green | 99.61 | 33.42 |
| | Blue | 99.62 | 33.45 |
| | Average | 99.62 | 33.46 |
| Baboon | Red | 99.57 | 33.48 |
| | Green | 99.64 | 33.59 |
| | Blue | 99.62 | 33.52 |
| | Average | 99.61 | 33.45 |
| Tapi | Red | 99.57 | 33.13 |
| | Green | 99.55 | 33.07 |
| | Blue | 99.56 | 33.07 |
| | Average | 99.56 | 33.09 |

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{29}$$

$$\text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\|C_1(i,j) - C_2(i,j)\|}{255} \times 100\% \tag{30}$$

With

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{31}$$

Where $C_1$ and $C_2$ denote two different levels of image encryption. $M, N$ make up the total number of image pixels. According to the optimal holding values, the NPCR threshold denoted as $N_\alpha^*$, while the UACI should remain within the designated critical range $(U_\alpha^* - \Delta, U_\alpha^* + \Delta)$. This can be expressed through the following equations:

$$N_\alpha^* = \frac{Q - \Phi^{-1}(\alpha)\sqrt{Q/H}}{Q+1} \tag{32}$$

### *4.3. Sensitivity key*

Key sensitivity is an essential property of a secure image encryption scheme, as even a very small variation in the secret key should lead to a completely different decryption result. This property ensures strong resistance against brute-force and key-approximation attacks. To evaluate the key sensitivity of the proposed method, a slight modification of $10^{-15}$ was introduced into the chaotic map parameters while keeping all other parameters unchanged. The objective was to verify whether such a minimal change could still allow successful decryption. The corresponding numerical results are presented in Table 8 and Table 9. Figure 12 and Figure 13 illustrate the decrypted images obtained using the correct secret key and a slightly modified key, respectively. The results clearly show that decryption with the modified key fails completely, producing a visually meaningless image. Quantitative analysis further confirms that more than 99.7% of the pixel values differ between the two decrypted images. These results demonstrate the high sensitivity of the proposed encryption scheme to its secret key parameters, thereby significantly enhancing its overall security.

Table 8. The responsiveness of the algorithm to a single pixel change in the original image

| | The correct key | The wrong key |
|---|---|---|
| Sine maps matrix | $\beta = 3.661185174124000$ | $\beta = 3.661185174123999$ |
| | $y_0 = 0.561425689012322$ | $y_0 = 0.561425689012322$ |
| First matrix of Logistic maps | $\alpha = 3.851725306782941$ | $\alpha = 3.851725306782941$ |
| | $x_0 = 0.754125612099426$ | $x_0 = 0.754125612099426$ |
| Second matrix of Logistic maps | $\alpha' = 3.994345671254013$ | $\alpha' = 3.994345671254013$ |
| | $x'_0 = 0.988123456813938$ | $x'_0 = 0.988123456813938$ |

Table 9. The percentage change rate (%)

| Parameter | Rate |
|---|---|
| $\beta$ | 99.514897 |
| $y_0$ | 99.593734 |
| $\alpha$ | 99.768829 |
| $x_0$ | 99.774169 |
| $\alpha'$ | 99.598185 |
| $x'_0$ | 99.614969 |


Figure 12. Key Sensitivity: (s1) Original Image (s2) Encrypted Image (s3) Decrypted Image with the correct key (s4) Decrypted Image with the wrong key

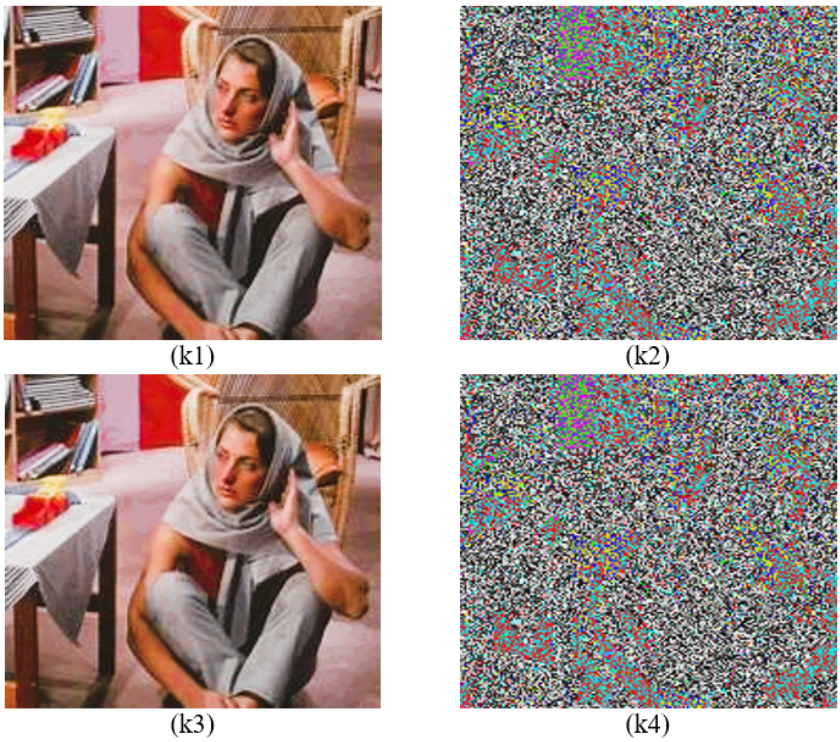



Figure 13. Key Sensitivity: (k1) Original Image (k2) Encrypted Image (k3) Decrypted Image with the correct key (k4) Decrypted Image with the wrong key

### *4.4. Entropy Analysis*

In image cryptography, entropy evaluates the unpredictability or disorder of pixels in an image. High entropy means that the image contains a lot of random information, making it harder to compress and predict. The confusion and diffusion phases used in encryption increase entropy, which increases the security of image encryption and protects sensitive visual data from malicious attacks[43] To calculate entropy, the following equation is used:

$$H(x) = \sum_{i=0}^{2^n-1} P(x_i) \log_2[1/P(x_i)] \tag{33}$$

With: $P(x_i)$ represents the probability of each $x_i$ occurring. In our context, we will assist the entropy of each color channel (blue, red and green), Therefore, there are 256 possible values for a pixel, which means that $n = 8$. When the source is totally unpredictable, the entropy $H(x)$ aims to achieve the value of 8. For each color channel (red, green, and blue), the results of our method's entropy calculation for the original and encrypted image are shown in Table 10 and Table 11 using various images. Additional techniques are also employed for comparison. The results obtained in Table 11 are close to the optimal value of 8. This suggests that our method can effectively withstand entropy attacks, thus exceeding the performance of the methods of El Azzaby et al.[39], Chen et al.[58] and Es-sabry et al.[41].

Table 10. The entropy of the secret and original images

| Image | Channel | Original Image | Encrypted Image |
|---|---|---|---|
| Lena | R | 7.25310 | 7.99940 |
| | G | 7.59403 | 7.99928 |
| | B | 6.96842 | 7.99924 |
| | Avg | 7.27185 | 7.99931 |
| Bird | R | 6.58497 | 7.99931 |
| | G | 6.71184 | 7.99929 |
| | B | 6.88567 | 7.99928 |
| | Avg | 6.72749 | 7.99929 |
| Baboon | R | 7.70667 | 7.99924 |
| | G | 7.47443 | 7.99920 |
| | B | 7.75221 | 7.99927 |
| | Avg | 7.64444 | 7.99923 |
| Peppers | R | 7.43501 | 7.99933 |
| | G | 7.65288 | 7.99939 |
| | B | 7.12658 | 7.99933 |
| | Avg | 7.404827 | 7.99935 |

Table 11. The Entropy comparison with other methods

| Image | Channels | Our Method | El Azzaby et al.[39] | Chen et al.[58] | Es-sabry et al.[41] |
|---|---|---|---|---|---|
| Lena | Red | 7.99940 | - | 7.99942 | 7.99903 |
| | Green | 7.99928 | - | 7.99929 | 7.99948 |
| | Blue | 7.99924 | - | 7.99929 | 7.99940 |
| | Average | 7.99931 | 7.99884 | 7.99933 | 7.99940 |
| Baboon | Red | 7.99924 | 7.99988 | - | 7.99895 |
| | Green | 7.99920 | 7.98852 | - | 7.99834 |
| | Blue | 7.99927 | 7.99910 | - | 7.99816 |
| | Average | 7.99923 | 7.99917 | - | 7.99861 |

### *4.5. Key Space Analysis*

The security of a chaos-based encryption algorithm strongly depends on the size of its key space. In the proposed method, the secret key is composed of the initial conditions and control parameters of the chaotic maps involved in the encryption process. Specifically, the secret key includes the initial condition $x_0, x_0'$ of the Sine map, the adaptive control parameter $R$ derived from the image variance, the initial condition $y_0$ and control parameter $\alpha_1$ of the first Logistic map, and the initial condition $z_0$ and control parameter $\alpha_2$ of the second Logistic map. Assuming a computational precision of $10^{-15}$ for each parameter, the total key space can be estimated as:

$$\text{KeySpace} = (10^{15})^7 = 10^{105} \approx 2^{349} \tag{34}$$

This key space is significantly larger than the minimum security threshold of $2^{128}$, making the proposed encryption scheme highly resistant to brute-force attacks.

### *4.6. Resistance to Known Attacks*

The proposed encryption algorithm demonstrates strong resistance against several well-known cryptographic attacks. In the case of chosen-plaintext attacks, the adaptive control parameter $R$ is derived from the variance of the input image. Any slight modification in the plaintext image leads to a different value of $R$, resulting in entirely different chaotic sequences and encrypted outputs. For known-plaintext attacks, the use of block-wise permutation with unique indices generated by Logistic maps, combined with XOR operations using sequences generated from intermediate encrypted images, makes it extremely difficult to establish any deterministic relationship between the plaintext and ciphertext. Moreover, the large key space and high key sensitivity provide strong resistance against brute-force attacks. These characteristics confirm the robustness of the proposed scheme against classical cryptanalytic attacks.

### *4.7. MSE and PSNR analysis*

MSE (Mean Squared Error) and PSNR (Peak Signal-to-Noise Ratio) are two frequently utilized metrics for evaluating image quality, particularly in the context of image encryption. The MSE calculates the average error square difference between the encrypted (or decrypted) image and the original image's equal pixel values. A robust encryption requires a considerable difference between the original image and the encrypted one, which is shown by a high MSE. PSNR is used to assess how well the image was reconstructed by comparing the encrypted (or decrypted) version to the original. It is measured in decibels (dB) and is based on the MSE. A low PSNR usually indicates better data protection. These two values are calculated between an encrypted image and the original image using the following equations:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - K(i,j)]^2 \tag{35}$$

$$\text{PSNR} = 10 \log_{10} \left( \frac{L^2}{\text{MSE}} \right) \tag{36}$$

With: $M$ and $N$ are the image size. $I(i,j)$ the value of the pixel at the position $(i,j)$ in the original picture. $K(i,j)$ the value of the pixel at the position $(i,j)$ in the encrypted image. $L$ is the largest possible value of a single pixel in the image.

Table 12. PSNR and MSE values for each of the encrypted and unencrypted images

| Image | Channels | Encrypted | | Decrypted | |
|---|---|---|---|---|---|
| | | MSE | PSNR | MSE | PSNR |
| Lena | R | 10666.86 | 7.861456 | 0 | Inf |
| | G | 9019.75 | 8.547459 | 0 | Inf |
| | B | 7168.05 | 9.563376 | 0 | Inf |
| | Avg | 8918.02 | 8.602030 | 0 | Inf |
| Airplane | R | 9940.78 | 8.156597 | 0 | Inf |
| | G | 10718.81 | 7.829336 | 0 | Inf |
| | B | 10498.69 | 7.919449 | 0 | Inf |
| | Avg | 10386.09 | 7.966279 | 0 | Inf |
| Baboon | R | 8682.46 | 8.744374 | 0 | Inf |
| | G | 7754.73 | 9.235132 | 0 | Inf |
| | B | 9488.07 | 8.359023 | 0 | Inf |
| | Avg | 8641.75 | 8.764783 | 0 | Inf |
| Peppers | R | 7994.55 | 9.102863 | 0 | Inf |
| | G | 11240.70 | 7.622868 | 0 | Inf |
| | B | 11126.85 | 7.667086 | 0 | Inf |
| | Avg | 10120.70 | 8.078697 | 0 | Inf |

Table 12 summarizes the outcomes from the values of MSE and PSNR for the 3 channels (blue, green and red) of the original and encrypted images before and after the encryption process. The values presented above confirm the efficiency and robustness of our encryption algorithm. The experimental results provide clear evidence of the proposed encryption technique's capability to protect color images. The histogram uniformity produced, the significant results for the correlation coefficient near zero, the high entropy, and the NPCR and UACI results all indicate the resistance of the method to both statistical and differential attacks. Using two Logistic maps is an essential way to effectively increase the level of diffusion, as they help remove all residual correlation effects. The first logistic map provides a high level of randomness, while the second logistic map increases all the randomization of small perturbations and spreads them uniformly in the ciphertext. The second Logistic map acts as a layer of diffusion to validate the need for using two Logistic maps in this method to increase the overall performance of the proposed method's security.

## 5. Future work

Future research will primarily focus on eliminating any remaining limitations present in the current proposed encryption scheme while also expanding its scope to include more current and standardized (advanced-level) forms of security protocols. To begin with, the processing speed of the algorithm being proposed will be improved through researching parallel implementations based upon GPU architecture and multi-core processors, which would allow for improved execution speeds while enabling the possibility of encrypted real-time streaming of high-quality color images and video. Then, as a second step, the research will consist of comparing the proposed chaos-based encryption scheme to standardized forms of encryption algorithms (i.e., Advanced Encryption Standard (AES)) that have been used in previous studies and papers. The outcome of this empirical analysis will provide a baseline comparison between the proposed scheme and other commonly utilized systems relative to levels of security strength, diffusion characteristics, functional effectiveness, etc. Third, in order to satisfy post-quantum security requirements, the proposed encryption framework will take a hybrid approach to encrypting data using chaos-based systems and quantum-resistant cryptographic primitives (eg, lattice and hash). In doing so, this combination will allow us to take advantage of the lower complexity and improved sensitivity that chaotic systems offer while

protecting against the potential threat posed by quantum attackers on current encryption technology. Fourth, several adaptive methods of generating a cryptographic key will be explored, where the chaotic parameters that define the key will be continually updated based on the data being processed and/or by evaluating additional sources of randomness, such as environmental fluctuations. These techniques are expected to significantly increase the resistance of the system to both known-plaintext and chosen-plaintext forms of attack. Finally, a comprehensive set of experiments will be completed using many different datasets and types of computing platforms to evaluate the scalability, robustness, and feasibility of using the proposed method to solve real-world problems, such as securely transmitting medical images, military communications, and IoT applications.

## 6. Conclusion

In this paper, a novel adaptive block-based encryption scheme for color images has been proposed using a combination of Sine and Logistic chaotic maps. In order to increase sensitivity to changes in plaintext, the encryption process uses an adaptive control parameter that is derived from the variance of the input image and works on non-overlapping 16x16 image blocks. While block-wise XOR operations with chaotic sequences created from intermediate encrypted images greatly reduce pixel correlation, the double application of logistic maps guarantees improved permutation and diffusion. Very low correlation coefficients, high entropy values close to the ideal value of 8, and strong defense against statistical and differential attacks are all demonstrated by experimental results. These results show that the proposed encryption method, which provides a high level of security while maintaining computational efficiency, is suitable for practical image security applications.

## Acknowledgement

This study receives backing from the National Scientific and Technical Research Center of Morocco. The completion of this paper is a part of project number 28/2020, funded under the Khawarizmi program.

REFERENCES

1. L. Kocarev and G. Jakimoski, "Logistic maps as a block encryption algorithm," *Physics Letters A*, vol. 289, pp. 199–206, 2001.
2. K. W. Wong, "A fast chaotic cryptographic scheme with dynamic lookup table," *Physics Letters A*, vol. 298, pp. 238–242, 2002.
3. N. K. Pareek, V. Patidar, and K. Sud, "Image encryption using chaotic logistic maps," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.
4. J. Wei, X. Liao, K. Wong, and T. Xiang, "A new chaotic cryptosystem," *Chaos, Solitons and Fractals*, vol. 30, pp. 1143–1152, 2006.
5. H. Yang, X. Lia, K. wo Wong, W. Zhang, and P. Wei, "A new cryptosystem based on chaotic map and operations algebraic," *Chaos, Solitons and Fractals*. In Press.
6. X. Wang and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 2, pp. 574–581, 2009.
7. G. Pastor, M. Romera, and F. Montoya, "A revision of the lyapunov exponent in 1d quadratic maps," *Physica D*, vol. 107, pp. 17–22, 1997.
8. K. Shahna and M. Anuj, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Applied Soft Computing*, vol. 90, p. 106162, 2020.
9. H. Huiqing, Y. Shouzhi, and Y. Ruisong, "Image encryption scheme combining a modified gerchberg–saxton algorithm with hyper-chaotic system," *Soft Computing*, vol. 23, pp. 7045–7053, 2018.
10. G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a chaotic encryption system," *Physics Letters A*, vol. 276, pp. 191–196, 2000.
11. C. Volos, I. Kyprianidis, and I. Stouboulos, "Text encryption scheme realized with a chaotic pseudo-random bit generator," *Journal of Engineering and Technology Review*, vol. 6, no. 4, pp. 9–14, 2013.
12. M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "Grayscale image encryption using shift bits operations," in *Int Conf Intell Syst Comput*, 2018.
13. M. Es-Sabry, N. El Akkad, M. Merras, A. Saaidi, and K. Satori, "A new color image encryption algorithm using random number generation and linear functions," in *Advances in Intelligent Systems and Computing*, vol. 1076, pp. 581–588, 2020.
14. V. Patidar, K. Sud, and N. Pareek, "A pseudo random bit generator based on chaotic logistic map and its statistical testing," *Informatica*, vol. 33, no. 4, pp. 441–452, 2009.
15. N. E. Ghouate, M. A. Tahiri, A. Bencherqui, *et al.*, "A high-entropy image encryption scheme using optimized chaotic maps with josephus permutation strategy," *Scientific Reports*, vol. 15, p. 29439, 2025.

16. M. Kumar, S. Kumar, R. Budhiraja, M. Das, and S. Singh, "A cryptographic model based on logistic map and a 3-d matrix," *Journal of Information Security and Applications*, vol. 32, pp. 47–58, 2017.
17. A. Wang and S. Gu, "New chaotic encryption algorithm based on chaotic sequence and plain text," *IET Information Security*, vol. 8, no. 3, pp. 213–216, 2014.
18. G. Jakimoski and L. Kocarev, "Analysis of some recently proposed chaos-based encryption algorithms," *Physics Letters A*, vol. 291, no. 6, pp. 381–384, 2001.
19. F. Elazzaby, N. E. Akkad, and S. Kabbaj, "Advanced encryption of image based on s-box and chaos 2d (lsmcl)," in *1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, 2020.
20. F. Elazzaby, N. E. Akkad, and S. Kabbaj, "New encryption approach based on four-square and zigzag encryption (c4cz)," in *Advances in Intelligent Systems and Computing*, vol. 1076, pp. 589–597, 2020.
21. H. Touil, N. E. Akkad, and K. Satori, "Text encryption: Hybrid cryptographic method using vigenere and hill ciphers," in *International Conference on Intelligent Systems and Computer Vision (ISCV)*, 2020.
22. G. Hu and B. Li, "Coupling chaotic system based on unit transform and its applications in image encryption," *Signal Processing*, vol. 178, p. 107790, 2021.
23. M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, 2020.
24. H. Touil, N. E. Akkad, and K. Satori, "H-rotation: Secure storage and retrieval of passphrases on the authentication process," *Int. J. Saf. Secur. Eng.*, vol. 10, pp. 785–796, Dec 2020.
25. H. Touil, N. E. Akkad, and K. Satori, "Secure and guarantee qos in a video sequence: A new approach based on tls protocol to secure data and rtp to ensure real-time exchanges," *Int. J. Saf. Secur. Eng.*, vol. 11, pp. 59–68, Jan 2021.
26. H. Touil, N. El Akkad, K. Satori, N. Soliman, and W. El-Shafai, "Efficient braille transformation for secure password hashing," *IEEE Access*, 2024.
27. F. Elazzaby, N. E. Akkad, K. Sabour, and S. Kabbaj, "An rgb image encryption algorithm based on clifford attractors with a bilinear transformation," in *Proc. Int. Conf. Big Data Internet Things*, pp. 116–127, 2022.
28. K. H. Sabour, S. Kabbaj, F. Elazzaby, and N. E. Akkad, "A new contribution of image encryption based on chaotic maps and the z/nz group," *Journal of Theoret. Appl. Inf. Technol*, vol. 101, pp. 37–47, Jan 2023.
29. F. Koulouh, S. Amine, M. Es-Sabry, *et al.*, "Optimizing color image security using hybrid cryptographic techniques based on sine and logistic maps," *Sci Rep*, 2026.
30. M. Es-Sabry, N. E. Akkad, M. Merras, A. Saaidi, and K. Satori, "A novel text encryption algorithm based on the two-square cipher and caesar cipher," in *Commun. Comput. Inf. Sci.*, vol. 872, pp. 78–88, Aug 2018.
31. F. Elazzaby, N. E. akkad, K. Sabour, and S. kabbaj, "A new encryption scheme for rgb color images by coupling 4d chaotic laser systems and the heisenberg group," *Multimed. Tools Appl.*, 2023.
32. F. Elazzaby, N. E. akkad, K. Sabour, W. El-Shafai, A. Torki, and S. Rajkumar, "Color image encryption using a zigzag transformation and sine–cosine maps," *Scientific African*, vol. 22, p. e01955, 2023.
33. W. Khedr, "A new efficient and configurable image encryption structure for secure transmission," *Multimed. Tools Appl.*, vol. 79, pp. 16797–16821, 2019.
34. O. E. ogri, H. Karmouni, M. Sayyouri, and H. Qjidaaa, "A novel image encryption method based on fractional discrete meixner moments," *Opt. Lasers Eng.*, vol. 137, p. 106346, 2021.
35. N. Singh and A. Sinha, "Chaos-based secure communication system using logistic map," *Optics and Lasers in Engineering*, vol. 48, pp. 398–404, 2010.
36. D. E. Goumidi and F. Hachouf, "Modified confusion-diffusion based satellite image cipher using chaotic standard, logistic and sine maps," in *2ème Atelier européen sur le traitement de l'information visuelle (EUVIP)*, (Paris, France), 2010.
37. H. Zeng and D. Chen, "Algorithme de chiffrement d'images basé sur le chaos composé logistic-sine," in *Conférence internationale 2020 sur l'informatique distribuée cybernétique et la découverte des connaissances (CyberC)*, (Chongqing, Chine), pp. 120–123, 2020.
38. P. Kiran and B. D. Parameshachari, "Logistic sine map (lsm) based partial image encryption," in *2021 National Computing Colleges Conference (NCCC)*, (Taif, Arabie Saoudite), pp. 1–6, 2021.
39. F. Elazzaby, N. Elakkad, and K. Sabour, "The coupling of a multiplicative group and the theory of chaos in the encryptions of images," *International Arab Journal of Information Technology*, vol. 21, no. 1, pp. 1–16, 2024.
40. M. Es-Sabry, N. E. 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.
41. M. Es-sabry, N. E. Akkad, L. Khrissi, K. Satori, W. El-Shafai, T. Altameem, and R. S. Rathore, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," *Egyptian Informatics Journal*, vol. 25, 2024.
42. X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.
43. M. Es-Sabry, N. E. Akkad, M. Merras, K. Satori, W. El-Shafai, T. Altameem, and M. M. Fouda, "Securing images using high dimensional chaotic maps and dna encoding techniques," *IEEE Access*, vol. 11, pp. 100856–100878, 2023.
44. M. El-Hajj, H. Mousawi, and A. Fadlallah, "Analysis of lightweight cryptographic algorithms on iot hardware platform," *Future Internet*, vol. 15, no. 2, p. 54, 2023.
45. X. Chai, J. Bi, Z. Gan, *et al.*, "Color image compression and encryption scheme based on compressive sensing and double random encryption strategy," *Signal Process.*, vol. 176, p. 107684, 2020.
46. K. Xuejing and G. Zihui, "A new color image encryption scheme based on dna encoding and spatiotemporal chaotic system," *Signal Process., Image Commun.*, vol. 80, p. 115670, 2020.
47. F. Koulouh, A. Safae, M. Es-Sabry, M. Mostafa, and N. Elakkad, "Optimization of grayscale image security through the use of hybrid cryptographic techniques based on sine and logistics maps," in *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, (FEZ, Morocco), pp. 1–7, 2024.

48. F. Kolouh, S. Amine, M. Es-sabry, and N. EL Akkad, "Enhancing data security through hybrid cryptographic techniques: Xor and rsa integration for rgb image encryption," in *Digital Technologies and Applications. ICDTA 2024*, vol. 1099 of *Lecture Notes in Networks and Systems*, Springer, Cham, 2024.
49. S. Amine, F. Koulouh, M. Es-sabry, and N. E. Akkad, "Image confidentiality through 1d chaotic map integration and shift operation," in *2024 International Conference on Circuit, Systems and Communication (ICCSC)*, (Fes, Morocco), pp. 1–7, 2024.
50. S. Amine, F. Koulouh, M. Es-sabry, and N. El akkad, "Securing visual data: A fresh approach with arnold cat map and chebyshev map encryption," in *Digital Technologies and Applications. ICDTA 2024*, vol. 1099 of *Lecture Notes in Networks and Systems*, Springer, Cham, 2024.
51. V. R. Folifack Signing, T. Fozin Fonzin, M. Kountchou, J. Kengne, and Z. T. Njitacke, "Chaotic jerk system with hump structure for text and image encryption using dna coding," *Circuits Systems Signal Process*, vol. 40, pp. 4370–4406, 2021.
52. M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for tmis based on elliptic curve integrated encryption and linear cryptography," *Multimed Tools Appl*, vol. 80, pp. 2081–2107, 2021.
53. S. Kandar, D. Chaudhuri, A. Bhattacharjee, and B. C. Dhara, "Image encryption using sequence generated by cyclic group," *Journal of Information Security and Applications*, vol. 44, pp. 117–129, 2019.
54. O. Faragallah, M. Alzain, H. El-Sayed, J. Al-Amri, W. El-Shafai, A. Afifi, E. Naeem, and B. Soh, "Block-based optical color image encryption based on double random phase encoding," *IEEE Access*, vol. 7, pp. 4184–4194, 2019.
55. L. Asghar, F. Ahmed, M. S. Khan, A. Arshad, and J. Ahmad, "Noise-crypt: Image encryption with non-linear noise, hybrid chaotic maps, and hashing," in *2023 International Conference on Engineering and Emerging Technologies (ICEET)*, (Istanbul, Turkiye), pp. 1–5, 2023.
56. Y. Wu, J. Noonan, and S. Agaian, "Npcr and uaci randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31–38, 2011.
57. J. Arif, M. Khan, B. Ghaleb, J. Ahmad, A. Munir, U. Rashid, and A. Al-Dubai, "a novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022.
58. J. Chen, J. Tang, F. Zhang, H. Ni, and Y. Tang, "a novel digital color image encryption algorithm based on a new 4-d hyper-chaotic system and an improved s-box," *Int. J. Innov. Comput. Inf. Control*, vol. 18, no. 1, pp. 73–92, 2022.