The Coupling of a Multiplicative Group and the Theory of Chaos in the Encryptions of Images

Fouzia Elazzaby
Department of Mathematics,
Ibn Tofail University, Morocco
fouzia099@hotmail.com

Nabil Elakkad
Laboratory of Engineering, Systems and Applications,
Sidi Mohamed Ben Abdellah University, Morocco
nabil.elakkad@usmba.ac.ma

Khalid Sabour
Department of Mathematics,
Ibn Tofail University, Morocco
khsabour2016@gmail.com

Abstract: *This study is centered on a significant scientific contribution within the realm of image cryptography. The chosen approach involves employing the bidimensional Arnold Cat Map transformation to reposition and modify pixel locations, guided by parameters derived from the original image. The construction of the multiplicative group Z/nZ, comprising equivalence classes modulo n, relies on a hyper-chaotic sequence derived from the 2D sinusoidal logistic modulation map. The correlation between this sequence and the preceding step yields an unpredictable blurring pattern, effectively altering the statistical properties of resulting matrices and distributing the influence of individual bits across the entire encrypted image. For each pixel, the encryption process entails an XOR operation with the Z/nZ group, followed by a right shift based on the three Least Significant Bits (LSB) of the preceding pixel. This meticulous procedure is iterated for every pixel, leaving no trace of similarity or association with the original plaintext image, effectively rendering it blurred and indecipherable. To gauge the efficacy of our algorithm, we subjected it to thorough evaluation utilizing diverse criteria, including histogram analysis, which unveiled a nearly uniform pattern in the encrypted images. Entropy values were found to be close to 8, while the correlation analysis exhibited a pronounced proximity to 0. Moreover, we subjected our approach to differential attacks, and the calculated values of the Number of Changing Pixel Rate (NPCR > 99.6) and the Unified Averaged Changed Intensity (UACI > 33.2) corroborated the strength and resilience of our methodology. In addition, to establish its comparative standing, we undertook a comprehensive assessment, meticulously comparing our method to various existing approaches from the literature, including those proposed by Hua, Es-sabry, and Faragallah. This systematic process accentuated the high level of responsiveness and sensitivity inherent in our approach, thus underscoring its innovative and promising nature.*

Keywords: *Image encryption, multiplicative group, map 2D-SLMM, security.*

Received September 8, 2022; accepted May 8, 2023
https://doi.org/10.34028/iajit/21/1/1

1. Introduction

The importance of images in contemporary media has reached unparalleled heights. The main reason for this can be attributed to the extensive usage of the W3, widespread access to computers, and the affordability of digital cameras and email [10]. Consequently, there has been an exponential surge in the sharing of graphical imagery and picture making. The application of images finds relevance and application in a wide spectrum of domains, encompassing endeavors such as: The development of a pioneering text encryption algorithm grounded in the principles of the two-square cipher and caesar cipher [11]. The establishment of a fresh methodology for color image encryption, which involves the generation of random numbers and the application of linear functions [13].

The utilization of shift bits operations for the encryption of grayscale images [14]. The introduction of an innovative approach to color image encryption, predicated on the generation of random numbers from two matrices and their subsequent manipulation using bit-shift operators [12]. The formulation of a distinct and efficient algorithm for reversible data hiding, specifically tailored for encrypted images with high capacity, while maintaining the reversibility of the process [23]. Additionally, the proliferation of smartphone cameras has resulted in a proliferation of mobile multimedia applications that employ cutting-edge technologies. Despite the relatively smaller size of images captured by the camera lens, there has been an astronomical rise in the volume of images being both captured and shared these cameras, millions of images are captured and shared on a daily basis worldwide, including documentation of significant and occasionally hazardous events. This necessitates the utmost attention from researchers to ensure secure transmission of across network infrastructures. [12, 15], thereby demanding the implementation of robust security techniques. Cryptography, in particular, strives to provide the most secure methods for image transmission [3, 28, 29, 34, 41]. However, their vulnerability to unauthorized attacks remains a concern despite the diversity of available methods. Furthermore, the field of image encryption continues to attract researchers who are exploring more effective approaches [1, 35, 37], as conventional encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are no longer suitable due to limitations in key space and the inability to guarantee message confidentiality. The challenges posed by image encryption lie in the massive data capacity and high pixel correlation, rendering most existing encryption techniques inadequate. Consequently, chaotic encryption techniques have gained prominence, characterized by properties such as susceptibility to initial conditions, nonperiodicity, topological transitivity, and pseudorandomness [5, 24, 33, 38]. Furthermore, chaotic encryption offers straightforward implementation and real-time image processing capabilities, making it applicable across various scientific disciplines. In light of these considerations, a state-of-the-art image encryption technique has been developed, founded on the principles of chaotic 2D Sine Logistic Modulation Map (2D-SLMM) maps. This method exhibits the capability to mimic the characteristics of a random signal, in this approach, a Z/nZ group is constructed, and it plays a pivotal role in modifying the pixel coordinates of the original image, leveraging the dynamics of the 2D-SLMM matrix. The resulting chaos-induced random shifts in pixel positions provide an intriguing mechanism for data concealment. The generated image then undergoes right horizontal diffusion, combining and shifting neighboring pixel properties to the right using the three least significant bits and the XOR operation. The effectiveness of this methodology was evaluated through various assessment measures, comparing it to existing methodologies [12, 20, 32, 43]. The experimental findings unequivocally showcase the exceptional resilience and effectiveness of our proposed technique in thwarting unauthorized access attempts

The structure of this study comprises an introduction, followed by a section describing the current state of the field. The proposed methodology is detailed in the subsequent section, while the experimental results illustrating the effectiveness and performance of the technique are presented in the fourth section. The study concludes with a summary in the concluding section.

2. Related Work

The literature encompasses various forms of cryptography [7, 8, 9, 22, 45], wherein the security of present-day data relies on computational algorithms whose secrecy is contingent upon the length of the key expressed in bits. However, the increasing computational power poses a threat to the confidentiality of traditional cryptographic methods. In the past decade, chaos theory has emerged as a technique to address this concern [4, 6, 19, 19, 27, 40].

Chaos theory involves employing different types of playing cards, including 1D chaotic maps characterized by a single variable and several parameters. The logistic, Gaussian, sine, and tent maps exhibit simple structures and chaotic orbits. However, the application of these maps is restricted due to their vulnerabilities, particularly regarding security. Technological advancements enable the estimation of chaotic signals, allowing the extraction of limited information as orbits and encryption parameters can be predicted. Consequently, several algorithms based on these maps prove to be insecure. For instance, Talhaoui *et al*. [36] introduced a novel image encryption scheme built upon the One-Dimensional Cosine Polynomial (1-DCP) map. This scheme combines permutation and substitution steps to enhance encryption speed and security. The 1-DCP map, defined by a straightforward iterative mathematical equation, exhibits highly chaotic behavior across a wide range of its positive real control parameters, as demonstrated by several analytical tests.

Additionally, there are high-performance chaotic [HD] cards that boast more intricate structures. The complexity of their orbits poses a challenge in predicting their behavior, making them fragile and susceptible to vulnerabilities. However, the implementation of these maps is known to be relatively arduous and resource-intensive.

Guo *et al*. [18] introduced a notable contribution in the domain of chaotic digital image encryption by proposing a general condition for quadratic functions. This condition aids in generating pseudo-random sequences that enhance the security of the encryption process. The approach involves topologically conjugating quadratic functions with both the logistic map and the tent map, resulting in a robust and dynamic encryption framework.

On a different front, Mansouri and Wang [30] developed an image encryption algorithm that leverages the Arnold map as its foundation. By incorporating split operations, rotation, and pixel scrambling, they elevated the algorithm's performance significantly. The revisions made to the map yielded noteworthy improvements in terms of both cost-effectiveness and complexity, making it an attractive option for image encryption applications.

Furthermore, Wang *et al*. [40] explored the potential of chaotic maps in conjunction with the Time-Delay Embedding Random Chaotic Sequence (TD-ERCS) system to generate two random sequences. This innovative approach holds the promise of enhancing the security and unpredictability of encryption techniques, paving the way for further advancements in the field.

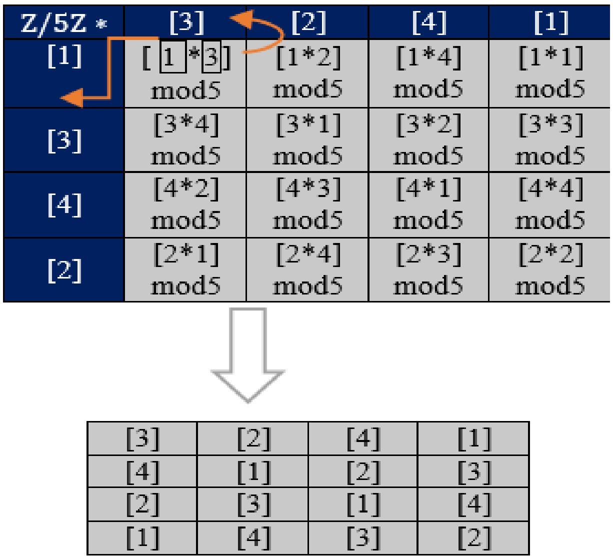
Hua *and* Zhou [21] employed models with a single dimension and a One-Dimensional Nonlinear Model (1D-NLM). These new cards are deemed more effective than current chaotic cards due to their greater capacity, unpredictable outputs, and adaptable attractor effects. Mollaeefar *et al*. [31] based their chaotic playing cards on color image encryption, providing high levels of security with rapid computations, reduced pixel correlation, and enhanced speed. Zhu *et al*. [46] utilized an analysis and simulation-based high-security technique that encrypts a plain image into a two-dimensional local binary pattern. The performance of the proposed algorithm and the effectiveness of the chaotic maps determine the system's security, as demonstrated by Belzani *et al*. [2], who employed algebraic analysis to decipher chaotic systems based on an RGB color scheme and DNA encoding. Chaotic trajectories depend on both time and information, necessitating the use of chaotic modulation to reinforce communication systems and improve the efficacy of chaotic maps. In summary, this method proves highly effective for secure communication.

3. The Mathematical Tools Employed in the Novel Scheme

3.1. The Group $\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$

Let us consider the integer variable ‘n’, which represents a non-negative value.

The group Zn/Z is defined as the set of equivalence classes. Each equivalence class represents a set of integers that are congruent to each other modulo n. For example, in the group Z5/Z, we will have the equivalence classes [0], [1], [2], [3], [4], where each class represents all integers congruent to 0, 1, 2, 3, or 4 modulo 5, respectively. Therefore, in this specific case, r ∈ {1, …, n-1} = r ∈ {1, …, 4}, as illustrated in Figure 1.



Z/5Z *	[3]	[2]	[4]	[1]
[1]	[1*3] mod5	[1*2] mod5	[1*4] mod5	[1*1] mod5
[3]	[3*4] mod5	[3*1] mod5	[3*2] mod5	[3*3] mod5
[4]	[4*2] mod5	[4*3] mod5	[4*1] mod5	[4*4] mod5
[2]	[2*1] mod5	[2*4] mod5	[2*3] mod5	[2*2] mod5

[3]	[2]	[4]	[1]
[4]	[1]	[2]	[3]
[2]	[3]	[1]	[4]
[1]	[4]	[3]	[2]

Figure 1. Example of constructing the Z5/Z group.

- **Commentary:** in the preceding example, we exclusively focused on utilizing the invertible elements within the algebraic structure of Z/5Z, specifically limited to the elements 1, 2, 3, and 4. This selective approach allowed us to explore and demonstrate the essential properties and operations of these elements in the context of the given scenario. By confining our examination to these specific elements, we were able to gain valuable insights into their interactions and mathematical properties, contributing to a comprehensive understanding of their significance within Z/5Z.

The equivalence class of an integer ‘x’, denoted as ‘[x]’, refers to a subset of the integer set ‘Z’ consisting of integers in the form ‘n + x’, where ‘k’ is an element of the set of integers (‘Z’). In the ensuing discourse, we expound upon the representation of the equivalence class of variable ‘x’ denoted by the remainder ‘r’, which spans from 0 to ‘n-1’. This representation is achieved through the utilization of Euclidean division of ‘x’ by ‘n’. Moreover, we adopt the succinct notation ‘x mod n’ to symbolize the said equivalence class of ‘x’.

In order to institute a multiplicative operation within the set ‘$\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$’, we propose that the product of the equivalence classes ‘(x mod n)’ and ‘(y mod n)’ equals the equivalence class of the product of ‘x’ and ‘y’, denoted as ‘xy mod n’.

However, it is important to note that when employing the aforementioned operation, the set ‘$(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^*$’, obtained by excluding the equivalence class representing 0 from ‘$\mathbb{Z}/\boldsymbol{n}\mathbb{Z}$’, does not generally form a group. Specifically, ‘$(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^{*}$’ constitutes a group only when the integer ‘n’ is a prime number. It is crucial to emphasize that for non-prime values of ‘n’, an equivalence class may not always possess an inverse element.

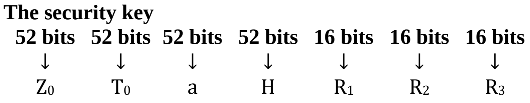
In the context of this study, our primary focus revolves around the prime number ‘n=257’. Therefore, the set ‘$((\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^*$, ×)’ constitutes a group, thereby encompassing a well-defined binary operation ‘×’ on the invertible elements within ‘$\mathbb{Z}/257\mathbb{Z}$’. Consequently, the invertible elements in the quotient group ‘$\mathbb{Z}/257\mathbb{Z}$' ' can be denoted and represented by the integers: 1, 2, 3, 4, 5, 6, 7, 8, ..., 255, and 256.

3.2. 2D Sine Logistic Modulation Map

The foundation of 2D-SLMM resides in the utilization of the Logistic and Sinus maps, serving as fundamental constituents. This enables the generation of a cartographic representation manifesting both sinusoidal oscillations and logistic progression or regression contingent upon the selected parameters. These maps are nonlinear functions renowned for their intricate and chaotic dynamics. Herein, we provide their explicit definitions.

$$\begin{cases} Z_{i+1} &= a(sin(\pi T_i)+b)Z_i(1-Z_i) \\ T_{i+1} &= a(sin(\pi Z_{i+1})+b)T_i(1-T_i) \end{cases} \quad (1)$$

By appropriately tuning the parameters a and b to specific values, namely a ϵ[0,1] and b ϵ[0,3], this operation is achieved through the utilization of a 256-bit secret key denoted as (Z_0, T_0, a, H, R_1, R_2, R_3). The precise structure of this secret key is visually represented in Figure 2.



The security key

52 bits	**52 bits**	**52 bits**	**52 bits**	**16 bits**	**16 bits**	**16 bits**
↓	↓	↓	↓	↓	↓	↓
Z_0	T_0	a	H	R_1	R_2	R_3

Figure 2. The structure of the security key.

The initial values (Z_0, T_0) and the control parameter a play a crucial role in the generation of the security key. Additionally, H, R_1, R_2 and R_3 are specifically designed to modify the initial conditions and parameters, thereby broadening the extent of the security key's coverage and enhancing its overall security.

To be more specific, Z_0, $T_{0,}$ a and H are decimal integers derived from a 52-bit string {b_1, b_2, …, b_{52}} utilizing the IEEE 754 format [33], as illustrated in Equation (2).

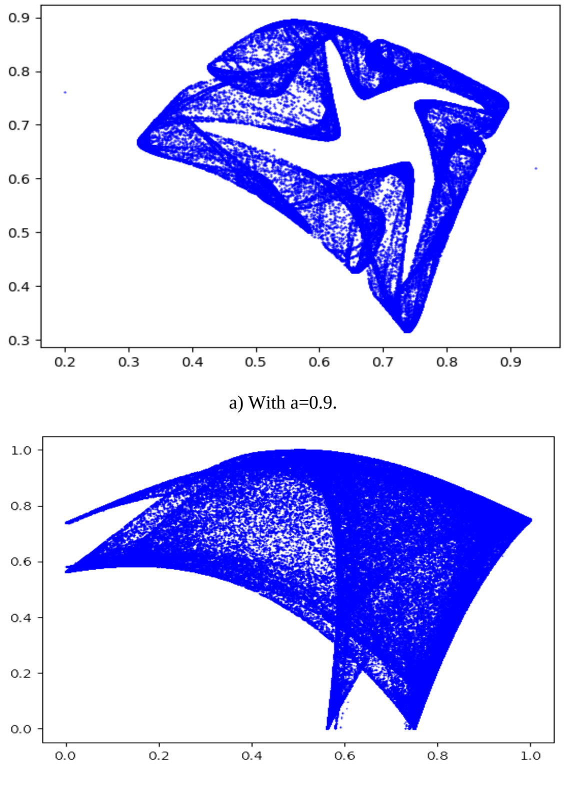
$$z = \frac{\sum_{i=1}^{52} b_i 2^{52-i}}{2^{52}} \tag{2}$$

Coefficients R_1, R_2, and R_3 are integers derived by the string {b1; b2; ..; b16}, which itself contains 16 bits. Two chaotic matrices, along with their initial values and the control parameters of 2D-SLMM, are defined by Equation (3)

$$\begin{cases} Z_{0i} & = & (Z_0 + R_i H) mod 1 \\ T_{0i} & = & (T_0 + R_i H) mod 1 \\ a_i & = & 0.9 + \left((a + E_i H) mod 0.1\right) \end{cases} \tag{3}$$

where *i* is either 1 or 3, and rounding is performed. Equation (3) prescribes the process of generating initial values limited to the range [0, 1], accompanied by the restriction that the control parameter 'a' lies within the interval [0.9, 1]. As a consequence, the 2D-SLMM showcases remarkable chaotic behavior when subjected to these specific values.

During our simulations, the security key is generated by employing a process of random bit stream generation.



a) With a=0.9.

b) With a=1.

Figure 3. The chaotic trajectory of 2D-SLMM.

Figure 3 shows the trajectory distributions of the 2D-SLMM system with the parameters respectively a=0.9 and a=1.when plotting these trajectory distributions, we can see that the trajectories of the 2D-SLMM in the region [0, 1]x[0, 1]reach a stable chaotic state.

4. The Proposed Technique

This section undertakes a thorough analysis of the inductive method employed in our pioneering encryption schema, which amalgamates 2D chaotic maps with principles from group theory.

In the initial phase, we commence by loading and extracting the three primary colors, namely R, G, and B, as illustrated in Figure 4, from the original image I. These colors are denoted by Ir, Ig, and Ib, respectively, with the following assignments: Ir=(:; :; 1); Ig=(:; :; 2); Ib(:; :; 3).

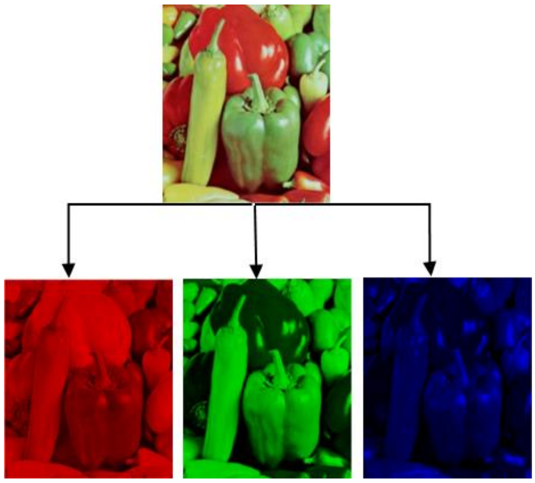


Figure 4. Extraction of the three planes R, G, and B from the image.

Next, we employ the three 2D chaotic matrices, generated by the 2D-SLMM, which will be elaborated on subsequently. These matrices possess a dimension of N×2. Each matrix is utilized to encrypt one of the three channels of the color image (Ir, Ib, and Ig), wherein the values of these channels are unique and fall within the range of 0 to 255.

4.1. The Encryption Process

Foremost in our methodological framework, we have incorporated the Arnold Cat Map as delineated in reference [30] to serve as the foundational element governing the confusion component. This intricate map constitutes a two-dimensional transformation specifically designed to operate on a 2x2 matrix, characterized by its determinant, which unequivocally equals 1. The salient utility of the Arnold Cat Map lies in its capacity to effectuate the systematic rearrangement and permutation of pixels extant within the confines of an image. This operation engenders a controlled and deliberate state of confusion, thereby manifesting a deliberate disruption of the image's spatial arrangement. The mathematical description of this transformative process is elucidated by means of Equation (4), serving as the precise formulation by which the Arnold Cat Map imparts its perturbing influence upon the image under consideration, thus constituting an indispensable facet of our comprehensive methodological approach.

$$\boldsymbol{\varphi}: \boldsymbol{P}\binom{\boldsymbol{u}}{\boldsymbol{v}} \to \boldsymbol{P'}\begin{pmatrix}(\boldsymbol{u}+\boldsymbol{Av})\ \boldsymbol{mod}\ \boldsymbol{N})\\ (\boldsymbol{Bu}+(\boldsymbol{AB}+\mathbf{1})\boldsymbol{v}\ )\ \boldsymbol{mod}\ \boldsymbol{N}\end{pmatrix} \qquad (4)$$

(u, v) represents the position of the pixels from the color image, A and B are an integer calculated for every channel (red, green, and blue), as depicted in Equations (5) and (6).

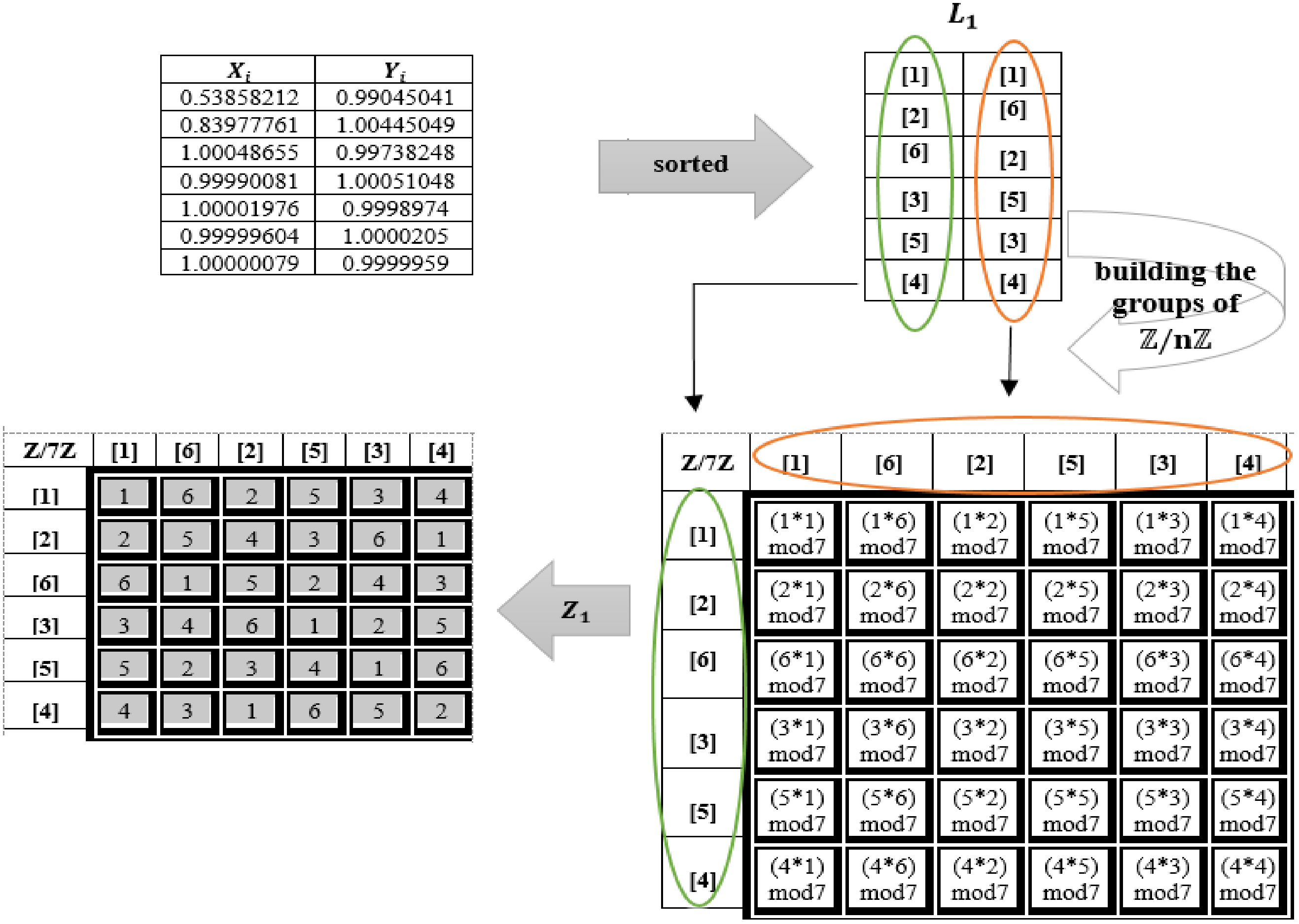
$$\boldsymbol{A} = \sum_{\boldsymbol{i,j}=\mathbf{1}}^{\boldsymbol{N}} \boldsymbol{I_k}(\boldsymbol{i},\boldsymbol{j})\ \boldsymbol{mod}\ \boldsymbol{N} \qquad (5)$$

$$\boldsymbol{B} = \mathbf{256} - \sum_{\boldsymbol{i,j}=\mathbf{1}}^{\boldsymbol{N}} \boldsymbol{I_k}(\boldsymbol{i},\boldsymbol{j})\ \boldsymbol{mod}\ \boldsymbol{N} \qquad (6)$$

During the decryption phase, we utilized the transformation outlined in Equation (7) to convert the scrambled image into the input image.

$$\begin{pmatrix}AB & -A\\ -B & 1\end{pmatrix}\binom{u'}{v'} = \binom{u}{v}\ mod\ N \qquad (7)$$

Next, we proceed to classify the three matrices generated using the chaotic map Equation (1) into separate rows. Subsequently, we construct three composite index matrices of size N×2, namely L1, L2, and L3, as illustrated in Figure 5. The matrix L1 is employed to compute the vector product within the multiplicative group $((\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^*, \times)$. Similarly, the application of matrix L2 enables the computation of the product of two arrays of elements within the multiplicative group $(\mathbb{Z}/\boldsymbol{n}\mathbb{Z})^*$, represented as Z2. Likewise, matrix L3 follows the same procedure for generating the product of two vectors, designated as Z3, within the aforementioned multiplicative group. Example of multiplication table in the set $\mathbb{Z}/7\mathbb{Z}$. x0=0.1245875, y0 = 0.6589444, a=1, b=3.



X_i	Y_i
0.53858212	0.99045041
0.83977761	1.00445049
1.00048655	0.99738248
0.99990081	1.00051048
1.00001976	0.9998974
0.99999604	1.0000205
1.00000079	0.9999959

L_1

[1]	[1]
[2]	[6]
[6]	[2]
[3]	[5]
[5]	[3]
[4]	[4]

Z/7Z	[1]	[6]	[2]	[5]	[3]	[4]
[1]	(1*1) mod7	(1*6) mod7	(1*2) mod7	(1*5) mod7	(1*3) mod7	(1*4) mod7
[2]	(2*1) mod7	(2*6) mod7	(2*2) mod7	(2*5) mod7	(2*3) mod7	(2*4) mod7
[6]	(6*1) mod7	(6*6) mod7	(6*2) mod7	(6*5) mod7	(6*3) mod7	(6*4) mod7
[3]	(3*1) mod7	(3*6) mod7	(3*2) mod7	(3*5) mod7	(3*3) mod7	(3*4) mod7
[5]	(5*1) mod7	(5*6) mod7	(5*2) mod7	(5*5) mod7	(5*3) mod7	(5*4) mod7
[4]	(4*1) mod7	(4*6) mod7	(4*2) mod7	(4*5) mod7	(4*3) mod7	(4*4) mod7

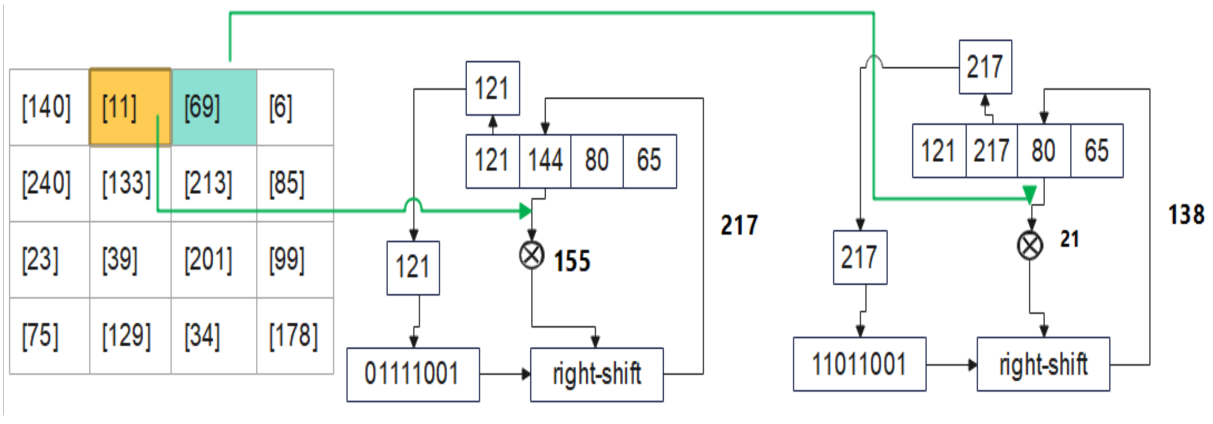
Z/7Z	[1]	[6]	[2]	[5]	[3]	[4]
[1]	1	6	2	5	3	4
[2]	2	5	4	3	6	1
[6]	6	1	5	2	4	3
[3]	3	4	6	1	2	5
[5]	5	2	3	4	1	6
[4]	4	3	1	6	5	2

Figure 5. An example of the construction of the group Z/nZ with the numbers generated by 2D-SLMM.

After the completion of constructing the sets of $\mathbb{Z}/\text{n}\mathbb{Z}$ groups (Z_1, Z_2, and Z_3), for every plane I_k, we apply a modification to the static characteristics of the image by dispersing the impact of each bit throughout the entire encrypted image. This effectively eliminates the possibility of differential attacks that involve comparing pairs of the original image and the encrypted image, except for the initial pixel. The initial pixel, however, is assigned the arithmetic sum of all the pixel values in the image, reduced modulo 256. Subsequently, each pixel is blended with the values from the multiplication groups Z1, Z2, and Z3, respectively, and then cyclically shifted to the right, adjacent to the decimal representation of the three least significant bits of the preceding pixel, as shown in Equation (8).

$$\begin{cases} \varphi'_k(1,1) = \sum_{i,j=1}^{256} \varphi_k(i,j)\%256 \\ \varphi'_k(i,j) = circshiftright\big(\varphi_k(i,j) \otimes Z_k(i,j)\big) \\ \varphi'_k(i+1,1) = \varphi_k(i+1,1) + Z_k(i,256), \\ \quad if\,(j-1 \neq 256 \; and \; (i,j) \neq (1,1)), \end{cases} \tag{8}$$

With *k=1, 2, 3*, the pixel values *φ1*, *φ2* and *φ3* are obtained after the rearrangement process detailed in the previous steps. A diagram, depicted in Figure 6, illustrates the process of right circular shift. Subsequently, the series of encrypted pixels pertaining to each plane undergoes a conversion process, wherein it is systematically arranged into an M×N matrix, resulting in the creation of the encrypted image.



(Z1)

a) The first iteration.

b) The second iteration.

Figure 6. Image equalization with the right horizontal diffusion process.

4.2. Process of Multiplicative Group and Chaos Theory in Image Encryption

In this particular section, we initiate a thorough and meticulous inquiry into the intricacies of the inductive methodology that finds application within the context of our pioneering encryption framework. This methodological scrutiny entails a nuanced exploration of the algorithmic underpinnings that facilitate the functioning of our innovative encryption system. At its core, this distinctive approach artfully synthesizes the multifaceted components of 2D chaotic mapping with the foundational tenets drawn from the discipline of group theory.

Within the purview of this comprehensive analysis, we aim to illuminate the inner workings of this fusion of disparate but synergistic elements. The employment of 2D chaotic maps introduces an element of stochastic complexity, fostering unpredictability and cryptographic robustness in our encryption mechanism. Concurrently, the incorporation of essential principles stemming from group theory imparts mathematical rigor and structural integrity to the framework, ensuring its resilience and soundness.

Algorithm 1: Pseudo Code for Multiplicative Group and Chaos Theory in Image Encryption

```
Input: Image P of size M x N and initial key ($x_0$,$y0$,$\alpha$,$H$,$Q_1$,$Q_2$,$Q_3$)
Output: Encrypted Image
Begin
- P: Input image data of size M x N x L
- L: Number of channels
- Pr, Pg, Pb: Individual color channels
1.  Extract the dimensions of the input image P:
   - M, N, L = size(P)
2.  Define color channels for the image:
   - channels L = {Pr, Pg, Pb}
3.  Generate three chaotic sequences using 2D-SLMM X1,
    Y1and Z1.
4.  Reshape the absolute values of the floor of Xi, Yi, and Zi
    modulo 256, which are generated from three chaotic
    sequences, into matrices respectively denoted as L1, L2,
    and L3, each of size [N, 2].
5.  Iterate through each channel and calculate the transformed
    value for $Z_k$ (i,j):
          $Z_k$ (i,j)= ($L_k$(i,1)$\otimes$ $L_k$ (j,2))mod
6.  Sequentially traverse through each individual channel, and
    proceed to compute the altered or metamorphosed value
    for $P_k$(i,j):
          $P_k$(i,j)= P(i+j,i+2*j)
7.  Calculate the sum of chaotic sequences for the current
    channel:
          $\varphi'_k(1,1) = \sum \varphi_k(i,j)$:
8.  Consecutively process each channel while computing the
    modified value for $\varphi'_k$ (i,j):
          $\varphi'_k(i,j) = circshiftright\big(\varphi_k(i,j) \otimes Z_k(i,j-1)\big)$
          $if\ (j-1 \neq 256\ and\ (i,j) \neq (1,1))$
          $\varphi'_k(i+1,1) = \varphi_k(i+1,1) + Z_k(i,256)$
  End Procedure
```

Subsequent to this meticulous dissection of our methodological approach, we commit to offering an illustrative elucidation of the envisaged procedural workflow. This exposition will manifest as a visual depiction, meticulously crafted in the form of a diagram. This graphical representation is conceived to serve as an invaluable didactic tool, facilitating the comprehension and assimilation of the proposed encryption procedure. The visual format, often recognized as a potent pedagogical device, promises to enhance the clarity and accessibility of our cryptographic innovation, empowering our audience with a lucid conceptual framework upon which to build their understanding, as depicted in Figure 7.

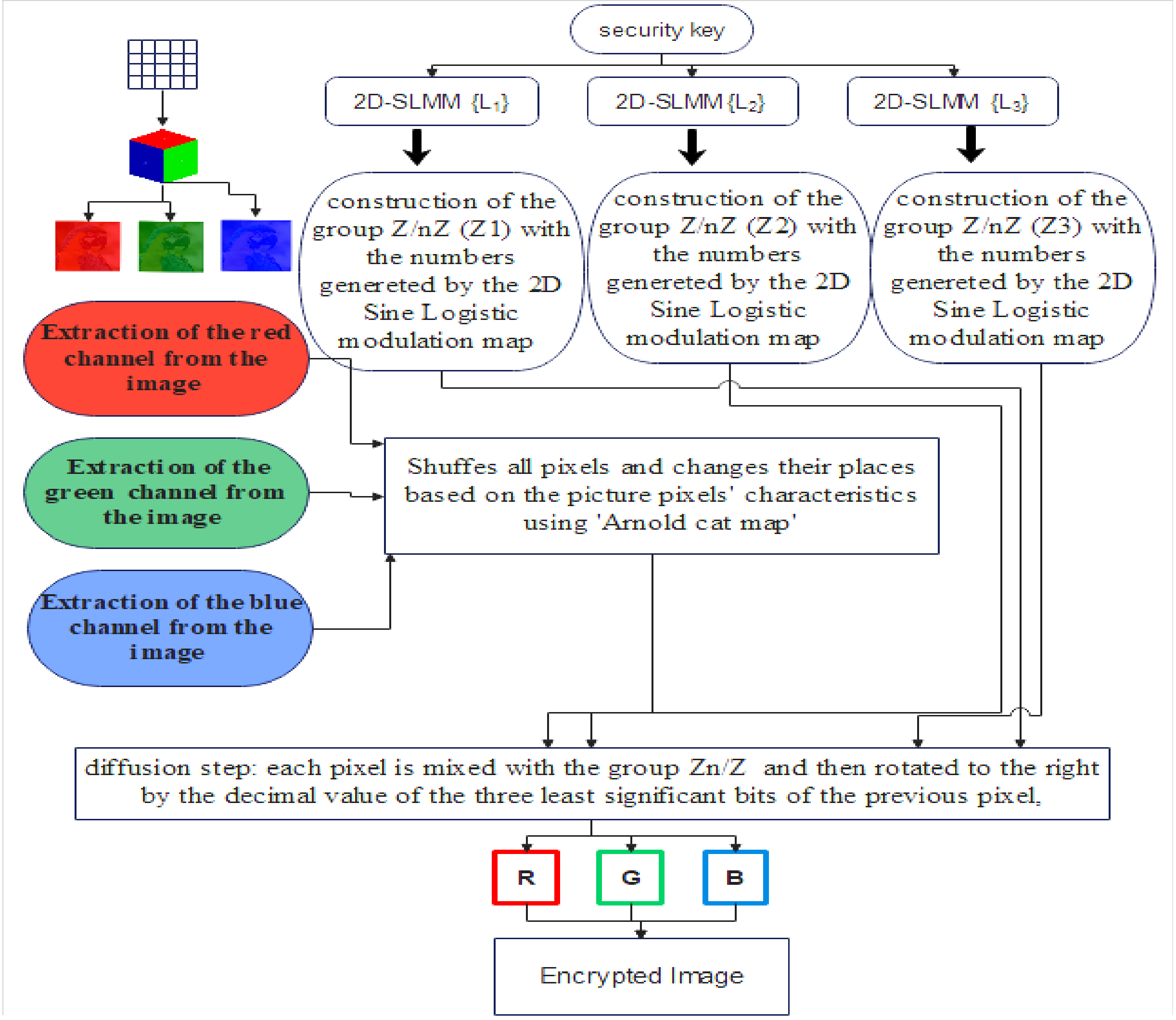

security key
2D-SLMM {L_1}
2D-SLMM {L_2}
2D-SLMM {L_3}
construction of the group Z/nZ (Z1) with the numbers genereted by the 2D Sine Logistic modulation map
construction of the group Z/nZ (Z2) with the numbers genereted by the 2D Sine Logistic modulation map
construction of the group Z/nZ (Z3) with the numbers genereted by the 2D Sine Logistic modulation map
Extraction of the red channel from the image
Extraction of the green channel from the image
Extraction of the blue channel from the image
Shuffes all pixels and changes their places based on the picture pixels' characteristics using 'Arnold cat map'
diffusion step: each pixel is mixed with the group Zn/Z and then rotated to the right by the decimal value of the three least significant bits of the previous pixel.
R
G
B
Encrypted Image

Figure 7. Flowchart of the proposed method.

5. Statistical Analysis

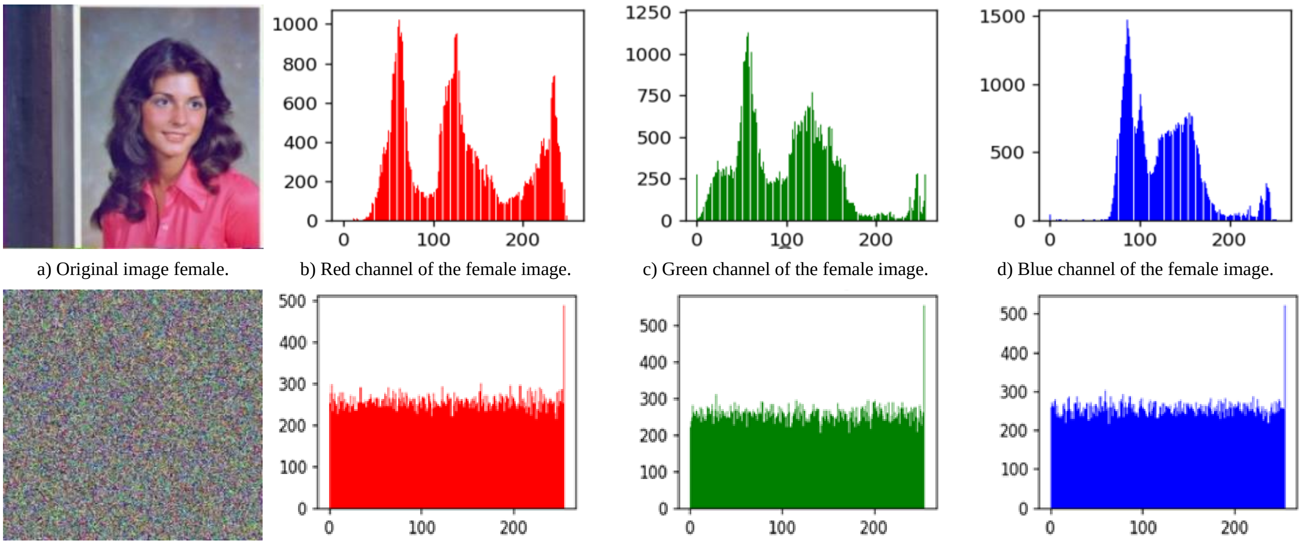
This section provides a thorough assessment of the efficacy and robustness of our proposed cryptographic primitive against unauthorized attacks documented in the existing literature. These attacks encompass statistical analysis, where cryptographic data is examining and interpreted using statistical methods. This involves analyzing patterns and other statistical properties of encrypted or decrypted data to derive insights or identify potential vulnerabilities. Additionally, brute force attacks are considered, which involve systematically exploring all possible combinations of keys or passwords until the correct one is discovered. It is important to note that brute force attacks are most feasible against encryption schemes that exhibit weak security and a limited key space.

To achieve this, we employed various security measures on six images sourced from the University of Southern California Signal and Image Processing Institute (USC-SIPI dataset), employing them as test images in our experiment, utilizing the Python programming language.

5.1. Histograms

The histogram is a commonly utilized measure to evaluate the graphical representation of intensity distribution in both encrypted and original images. In light of this, we have undertaken a comparative analysis of the histograms derived from eight distinct original images, each depicting dissimilar content, and the histograms of their corresponding encrypted counterparts, employing our innovative technique.

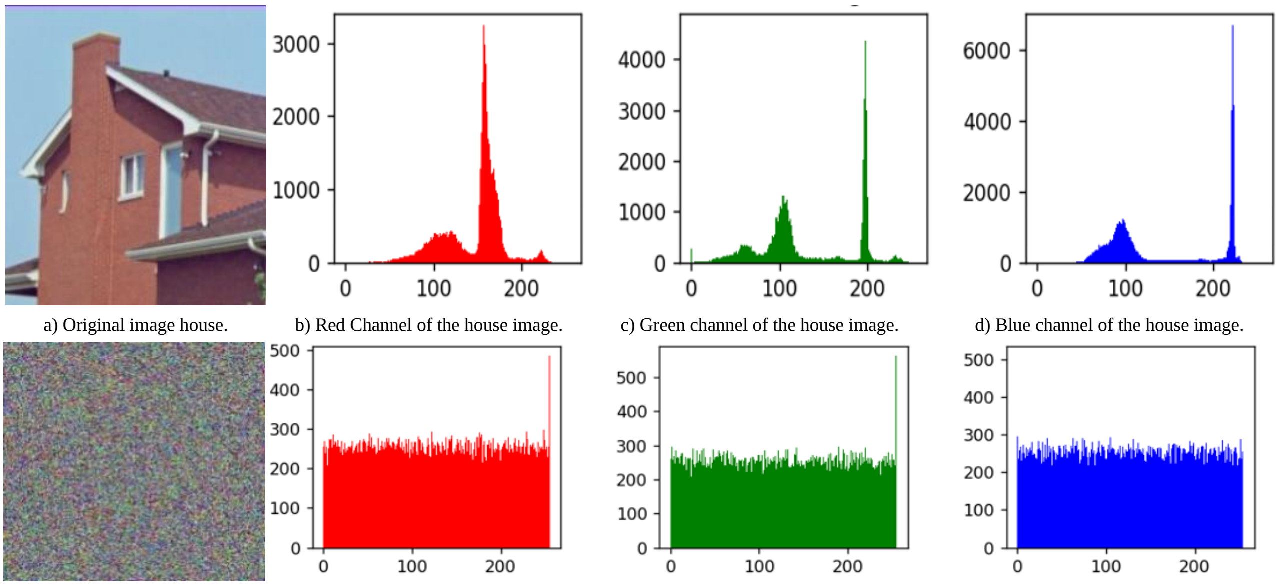
Upon careful examination of Figures 8, 9, 10, 11, 12, and 13, it became evident that the pixel distribution within the histograms of the encrypted images exhibited a near-uniform pattern. In contrast, the histograms of the original images displayed a notable disparity, characterized by significantly elevated values in certain regions and markedly lower values in others. This conspicuous dissimilarity observed between the two histograms reaffirms our assertion that our novel approach robustly ensures security by effectively safeguarding the images against statistical attacks.



a) Original image female. b) Red channel of the female image. c) Green channel of the female image. d) Blue channel of the female image.

e) Cipher image female. f) Cipher red channel of the female image. g) Cipher green channel of the female image. h) Cipher blue channel of the female image.

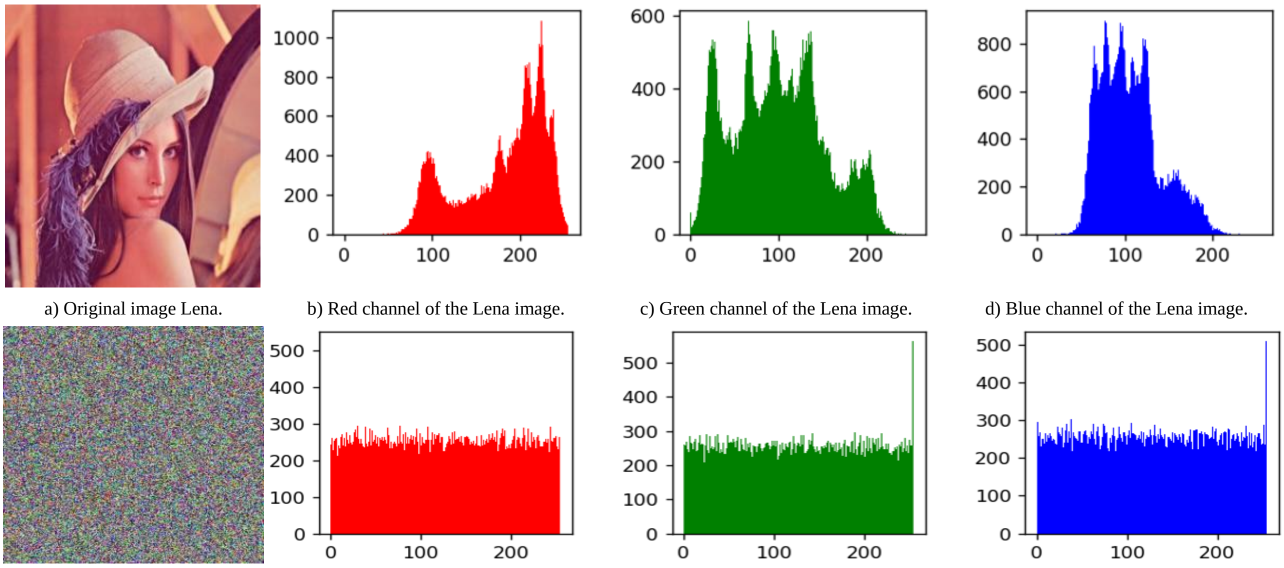
Figure 8. Histograms of the original female image and the encrypted version.



a) Original image house. b) Red Channel of the house image. c) Green channel of the house image. d) Blue channel of the house image.

e) Cipher image house. f) Cipher red channel of the house image. g) Cipher green channel of the house image. h) Cipher blue channel of the house image.

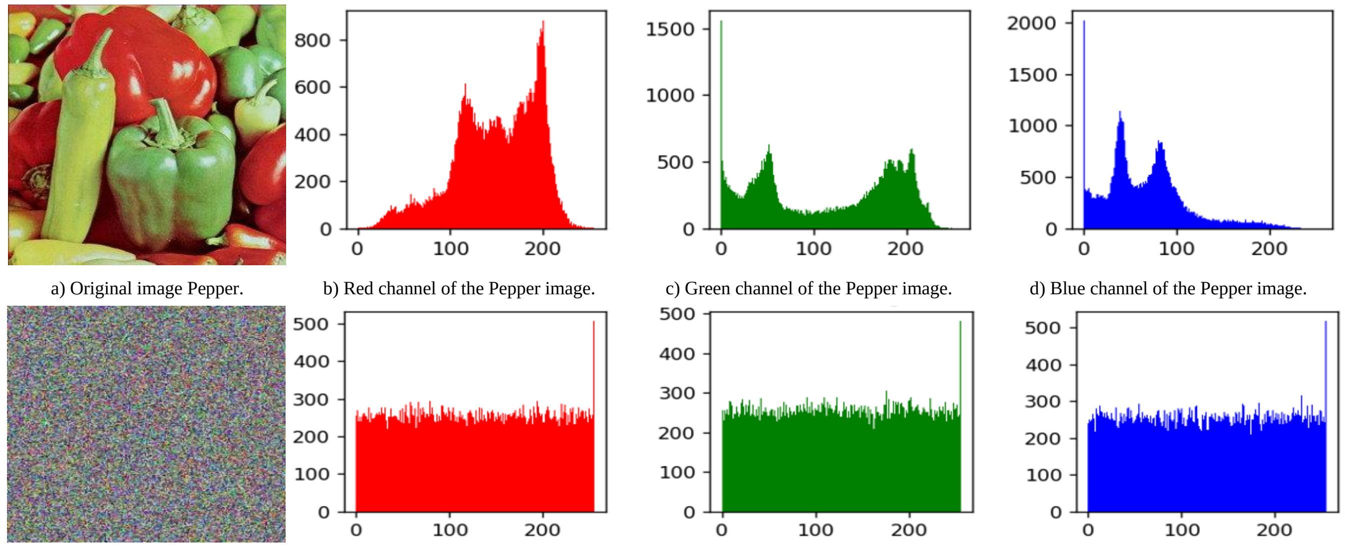
Figure 9. Histograms of the original house image and the encrypted version.



a) Original image Lena. b) Red channel of the Lena image. c) Green channel of the Lena image. d) Blue channel of the Lena image.

e) Cipher image Lena. f) Cipher red channel of the Lena image. g) Cipher green channel of the Lena image. h) Cipher blue channel of the Lena image.

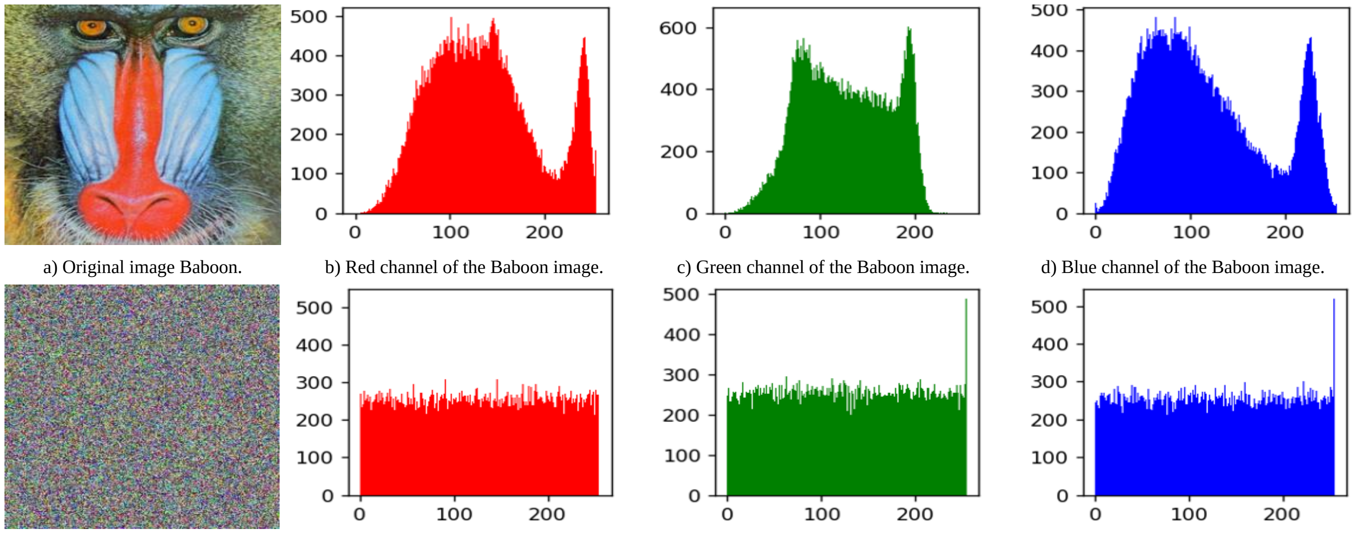
Figure 10. Histograms of the original Lena image and the encrypted version.



a) Original image Pepper. b) Red channel of the Pepper image. c) Green channel of the Pepper image. d) Blue channel of the Pepper image.

e) Cipher image Pepper. f) Cipher red channel of the Pepper image. g) Cipher green channel of the Pepper image. h) Cipher blue channel of the Pepper image.

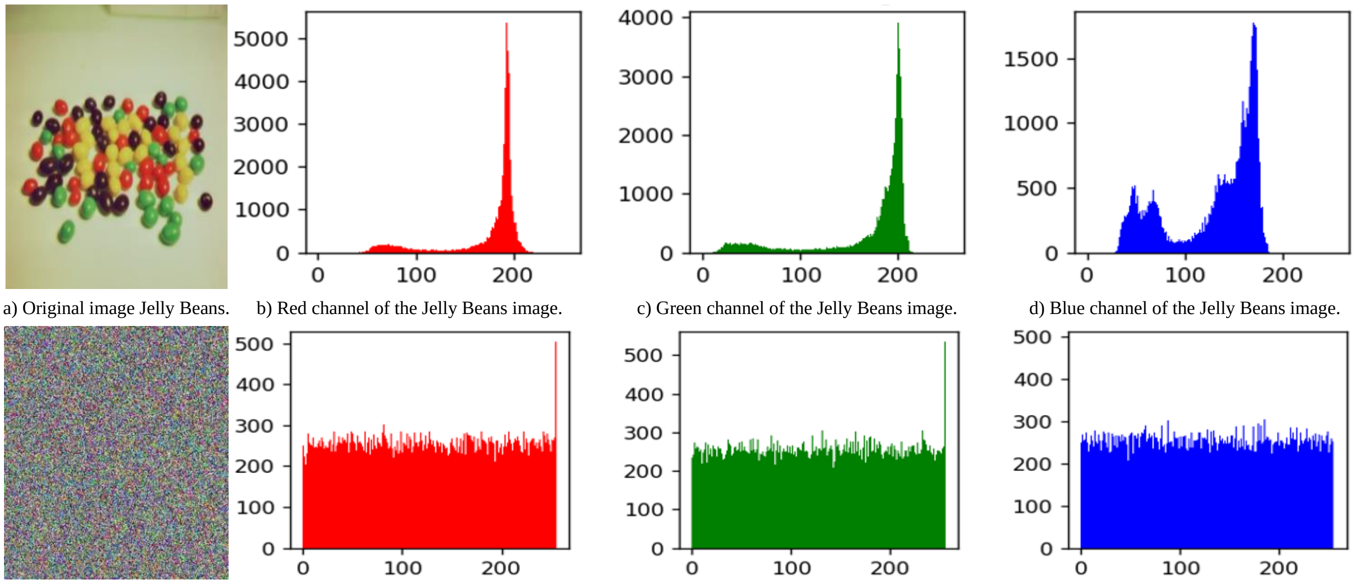
Figure 11. Histograms of the original Pepper image and the encrypted version.



a) Original image Baboon. b) Red channel of the Baboon image. c) Green channel of the Baboon image. d) Blue channel of the Baboon image.

e) Cipher image Baboon. f) Cipher red channel of the Baboon image. g) Cipher green channel of the Baboon image. h) Cipher blue channel of the Baboon image.

Figure 12. Histograms of the original Baboon image and the encrypted version.



a) Original image Jelly Beans. b) Red channel of the Jelly Beans image. c) Green channel of the Jelly Beans image. d) Blue channel of the Jelly Beans image.

e) Cipher image Jelly Beans. f) Cipher red channel of the Jelly Beans image. g) Cipher green channel of the Jelly Beans image. h) Cipher blue channel of the Jelly Beans image.

Figure 13. Histograms of the original Jelly Beans image and the encrypted version.

5.2. Coefficient of Correlation between two Adjacent Pixels

Each image consists of numerous crucial internal data bits that encompass the "correlation coefficient between neighboring pixels," making it vulnerable to statistical attacks. Therefore, it is essential to enhance the effectiveness of this coefficient while minimizing or eliminating it entirely to create original images that are exceptionally weak and exceedingly difficult to decipher. In order to achieve such a high level of security, an experimentation was conducted as described below: A comprehensive total of 5,000 pairs of adjacent pixels were randomly chosen from both the plain and encrypted images in three directions-horizontal, vertical, and diagonal. Following this selection process, the specified Equations (9), (10), (11), and (12) were employed to perform the computations on the images presented in Figures 8, 9, 10, 11, 12, and 13.

$$r_{xy} = \frac{\mathrm{Cov}(x, y)}{\sqrt{D_x}\sqrt{D_y}} \tag{9}$$

$$\mathrm{Cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E_x)(y_i - E_y) \tag{10}$$

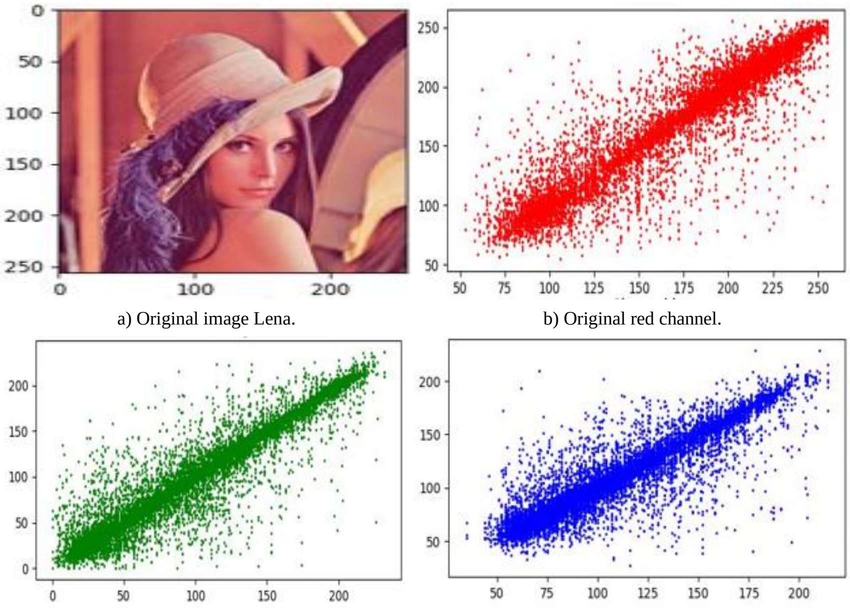
$$D_x = \frac{1}{N}\sum_{i=1}^{N} (x_i - E_x)^2 \tag{11}$$

$$E_x = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{12}$$

The coefficient value, denoted as r_{xy} ∈(-1,1), represents the degree of association between neighboring pixels, with "0" indicating no correlation and "1" indicating a strong correlation. Table 1 displays the correlation coefficients obtained from 5000 randomly selected pairs of adjacent pixels. Therefore, we observe that the measured correlation coefficient of the encrypted images in the different red, blue, and green channels, following the horizontal, vertical, and diagonal orientations respectively, using our novel approach, approaches zero. Indeed, despite a low correlation value, a significant correlation is observed between the correlation coefficients of the original and encrypted images. This indicates that the proposed technique is capable of withstanding statistical attacks.

Table 1. Coefficients of correlation between two neighboring pixels in the source-image and the cipher-image.

Image		Image Original			Encrypted Image		
	Channels	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
4.1.04	**Red**	0.9787226	0.9877570	0.9683581	0.0077581	-0.0056768	-0.0151963
	Green	0.9674671	0.9770061	0.9491186	-0.0033764	-0.0197305	-0.0086353
	Blue	0.9494685	0.9723321	0.9273325	0.0142651	0.0115167	0.0148024
	Average	0.96521941	0.97903171	0.94826972	0.00621560	-0.00463021	-0.0030097
4.1.05	**Red**	0.9634450	0.9393284	0.9093912	-0.0066705	-0.0107594	0.0198871
	Green	0.9794307	0.9517136	0.9355478	0.0099129	-0.0129709	-0.0004038
	Blue	0.9817456	0.9741091	0.9620894	-0.0040523	-0.0072853	0.0119220
	Average	0.974873791	0.9550503	0.93567615	-0.0002699	-0.0103385	0.0104684
4.2.07	**Red**	0.9466559	0.9519504	0.9153055	0.0170036	-0.0414627	0.0307309
	Green	0.9720316	0.9731752	0.9475762	0.0116373	-0.0072126	-0.0157430
	Blue	0.9450629	0.9498410	0.9090078	0.0079672	0.0259731	-0.0277482
	Average	0.954583460	0.95832219	0.92396316	0.0122026	-0.0075674	-0.0042534



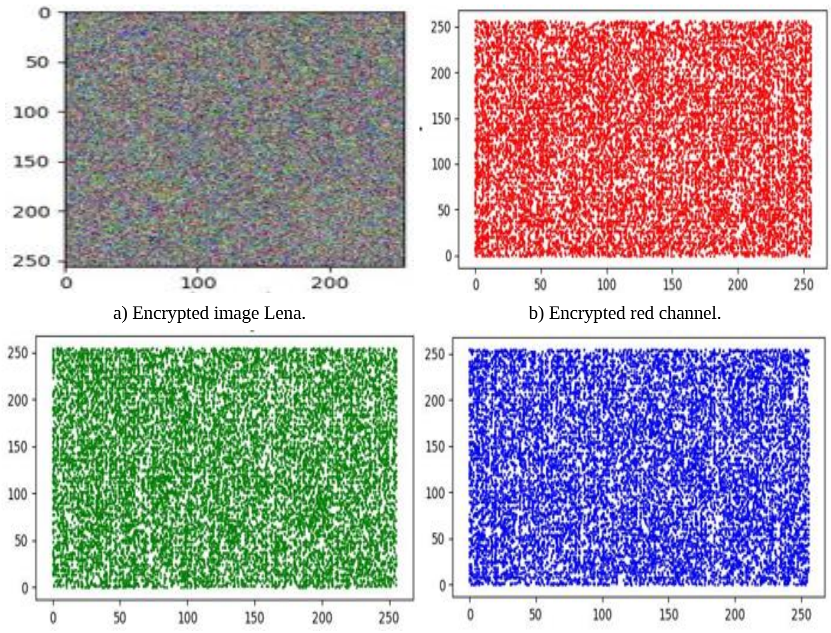
a) Original image Lena.

b) Original red channel.

c) Original green channel.

d) Original blue channel.

Figure 14. Coefficient of correlation between neighboring pixels in each channel of the Lena source picture.



a) Encrypted image Lena.

b) Encrypted red channel.

c) Encrypted green channel.

d) Encrypted blue channel.

Figure 15. Correlation coefficient of nearby pixels in each channel of the encrypted Lena picture.

Hence, we deduce that our methodology is notably proficient in disrupting the dependency among neighboring pixels, as illustrated by Figures 14 and 15.

Table 2. Comparison of correlation coefficients between two neighboring pixels in diverse orientations using the provided method and other algorithms.

Encrypted image	**Directions**			**Average**
	Horizontal	**Vertical**	**Diagonal**	
Hua *et al*. [22]	0.002383	0.008576	0.040242	0.017067
Tong *et al*. [37]	0.003800	0.005800	0.013300	0.007633
Es-Sabry *et al*. [12]	-0.007205	0.025854	-0.009817	0.002944
Faragallah *et al*. [16]	-0.0000667	0.0367	0.0247	0.020444
Proposed method	-0.0036073	0.0074088	-0.002342	0.0004865

According to the findings presented in Table 2, our method surpasses the depend-ability and performance levels achieved by Tong *et al*. [37], Faragallah *et al*. [16], Es-Sabry *et al*. [12], and Hua *et al*. [20]. Additionally, the results highlight the capability of our method to completely eradicate any semblance or similarity between the plain image and its encrypted counterpart.

5.3. Correlation Coefficient Analysis between the Original and Encrypted Images

It is important to emphasize that the aforementioned test was carried out with consideration to three orientations. However, in our analysis, the primary emphasis will be on computing the correlation coefficient for every pixel present in both the source image and the image designated for encryption, this will be accomplished by employing the Equations (13), (14), and (15), as shown below:

$$\mathrm{CC} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{ij}-\bar{I}\right)\left(I'_{ij}-\bar{I}\right)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{ij}-\bar{I}\right)^{2}}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I'_{ij}-\bar{I}\right)^{2}}} \tag{13}$$

$$\bar{I} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} I_{ij} \tag{14}$$

$$\bar{I}' = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} I'_{ij} \tag{15}$$

Let I denote the plain image and $\bar{I}$ represent its average. Similarly, I' corresponds to the ciphered image and $\overline{I'}$ represents its average. The dimensions of the matrices I and I' are represented by N (length) and M (width), respectively.

Table 3. Comparison of the correlation coefficient of our algorithm.

Encrypted image	**Channels**	**Our**	**Es-sabry *et al*. [12]**	**Wu *et al*. [43]**	**Faragallah *et al*. [16]**
Lena	**Red**	-0.00299787	0.007621	–	-0.0000667
	Green	0.00021103	0.005257	–	0.0367
	Blue	0.00424563	- 0.007645	–	0.0247
	Average	0.00048627	0.001744	0.002851	0.020444
Baboon	**Red**	0.0020906	0.002012	–	–
	Green	-0.00377277	0.007464	–	–
	Blue	0.00206403	0.008313	–	–
	Average	0.00012729	0.005929	−0.006632	–
Peppers	**Red**	0.00016207	0.014940	–	–
	Green	-0.00312463	- 0.020151	–	–
	Blue	0.00651457	0.002337	–	–
	Average	0.001184	- 0.001332	−0.001650	–

The Table 3 provides evidence of the exceptional performance of our methodology compared to the results obtained by the methodologies presented in [43], which introduce an innovative image encryption algorithm that seamlessly integrates the rectangular transform and the Chaotic Tent Map (CTM) principle. Furthermore, our approach surpasses the technique described in [12], which depends on generating random numbers from two matrices and utilizing bit-shift operators, as well as the method explained in [16]. This superiority can be attributed to the obtained values that demonstrate a remarkable proximity to zero

5.4. Differential Attacks

The cryptographic system exhibits resistance against a differential attack [44], which refers to a targeted assault on a chosen plain image with the objective of uncovering the secret key. A robust encryption method, whether symmetric or asymmetric, should display high sensitivity to slight modifications in the plain picture, resulting in significant alterations in the encrypted output, even with a minute change of a single bit in the input image. The sensitivity of the cryptosystem is measured using two metrics known as the Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) when observing the source images. To evaluate this, we took a photograph of Lena and made a minor adjustment to a single pixel. Subsequently, we calculated the NPCR and UACI using Equations (16) and (17) respectively, and obtained values exceeding 99.6% and 33.8% (refer to Tables 4 and 5). Furthermore, they demonstrate a higher level of efficiency when compared to alternative methodologies, as exemplified by Es-Sabri *et al*. [14], this method relies on the random generation of two matrices and the utilization of bit shift operators to encrypt a color image.

Table 4. Result of the algorithm's sensitivity to a modification in a single pixel of the source image.

Encrypted image	**Channels**	**Our**		**Es-Sabri *et al*. [14]**		**Hua and Zhou [21]**		**Wang and Guo [39]**	
		NPCR	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**	**NPCR**	**UACI**
Lena	**Red**	99.770056	33.481624	–	–	–	–	–	–
	Green	99.805151	33.697173	–	–	–	–	–	–
	Blue	99.728857	33.650470	–	–	–	–	–	–
	Average	99.768021	33.609756	99.67576	33.59832	99.60679	33.3741	99.6071	33.4692

Table 5. Results for NPCR and UACI of the suggested method.

Image	**Channels**	**NPCR**	**UACI**
4.1.02	**Red**	99.726486	33.479827
	Green	99.759375	33.694587
	Blue	99.707495	33.609754
	Average	99.734452	33.594723
4.1.04	**Red**	99.731909	33.555653
	Green	99.720383	33.644590
	Blue	99.780737	33.679530
	Average	99.747676	33.626591
4.1.05	**Red**	99.719702	33.795178
	Green	99.760900	33.561892
	Blue	99.713598	33.504208
	Average	99.731400	33.620426
4.2.03	**Red**	99.795996	33.803106
	Green	99.745642	33.581974
	Blue	99.698339	33.574715
	Average	99.746659	33.653265

Another example is Hua and Zhou [21], who proposes a 1D-NLM for processing chaotic sequences.

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\% \tag{16}$$

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

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j) \\ 1, & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \tag{17}$$

where *C1* and *C2* denote two different encrypted images. *MN* is the total number of image pixels. According to the ideal expectation values of NPCR is larger than the critical NPCR score N_α^* and its UACI falls into the critical UACI interval $(U_\alpha^{*-}, U_\alpha^{*+})$ using the following equations:

$$N_\alpha^* = \frac{Q - \Phi^{-1}(\alpha)\sqrt{Q/H}}{Q+1} \tag{18}$$

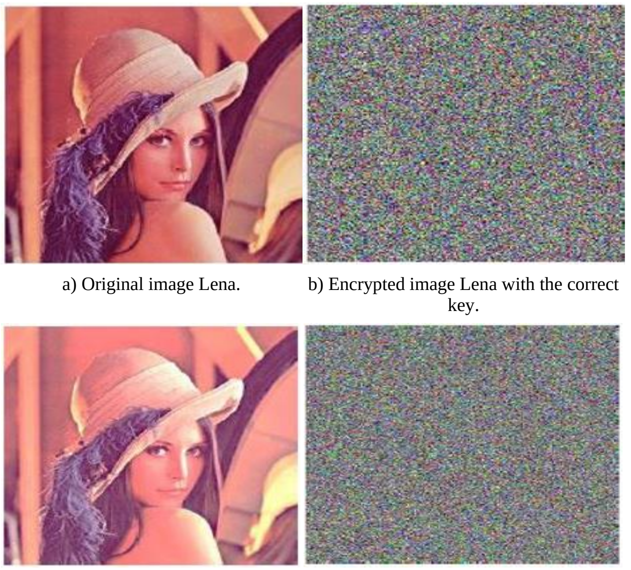
$$\begin{cases} U_\alpha^{*-} = \mu_u - \Phi^{-1}\left(\frac{\alpha}{2}\right)\sigma_u; \\ U_\alpha^{*+} = \mu_u + \Phi^{-1}\left(\frac{\alpha}{2}\right)\sigma_u, \end{cases} \tag{19}$$

5.5. Key Sensitivity

An essential characteristic of an optimal image encryption algorithm lies in its susceptibility to the private key, to the extent that even a minor modification in the private key should yield a wholly distinct image. Therefore, we conducted a comprehensive key sensitivity analysis for the proposed image encryption system to assess whether the decryption operation would successfully proceed in the event of a 10^{14} order alteration in a parameter of the chaotic functions employed in constructing the algorithm $\mathbb{Z}/n\mathbb{Z}$ group (refer to Table 6). Figures 16 and 17 present the outcomes of the decryption process, showcasing both the correct key and the modified key. These results unequivocally reveal that even a slight alteration in the key has led to a substantial transformation in the decryption.

Table 6. The algorithm's responsiveness to a modification in a single pixel of the plain image.

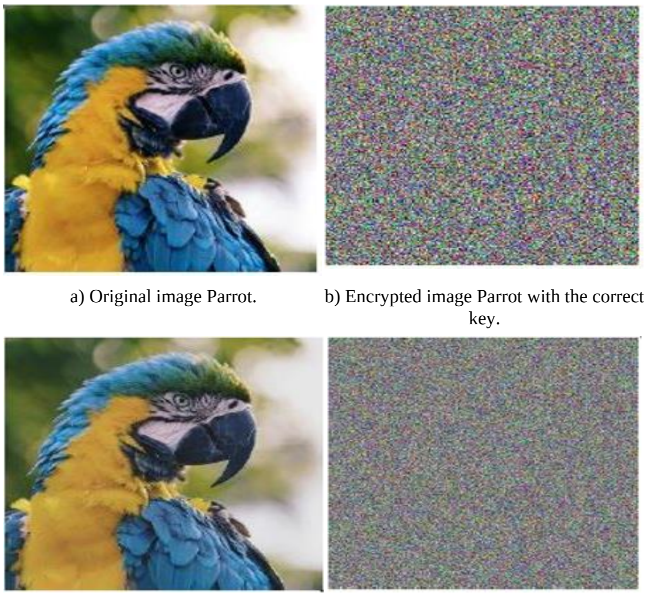
The correct key	**The wrong key**
X_0=0.17466775762309	X_0=0.17466775762310
Y_0=1.63135422500059	Y_0=1.63135422500059
a=0.6523510213	a=0. 6523510213
b=1.3629853012	b=1. 3629853013



a) Original image Lena. b) Encrypted image Lena with the correct key.

c) Decrypted image Lena with the correct key. d) Decrypted image Lena with the incorrect key.

Figure 16. Key sensitivity analysis of the encryption process for the Lena image.



a) Original image Parrot. b) Encrypted image Parrot with the correct key.

c) Decrypted image Parrot with the correct key. d) Decrypted image Parrot with the incorrect key.

Figure 17. Key sensitivity analysis of the encryption process for the parrot image.

5.6. Entropy Information

Entropy measures the amount of chaos caused by the encryption algorithm at its output and determines how unpredictable communication is. If the diffusion process is effective, we will have a significant degree of disorder in encrypted images [17]. Therefore, entropy becomes high. On the other hand, the randomness of the encryption process is insufficient, making the cryptosystem susceptible to an entropy attack since the encryption method is somewhat predictable. This section tests and verifies the effectiveness of the suggested encryption diffusion stage. Equation (20) can be used to determine a message's entropy *H(s)*:

$$H(s) = \sum_{i=0}^{2^n-1} P(s_i) log_2[P(s_i)] \qquad (22)$$

- $P(s_i)$ represents the probabilities associated with the occurrence of each individual *Si*.

The total number of states for the information source is represented by 2^n. Notably, the entropy is considered to be equal to 'n' for the random information source to be deemed perfect, possessing precisely 2^n states.

In our example, the computation is performed for each channel (red, green, and blue), therefore the number of states is 2n=256, and the ideal entropy is therefore n=8.

The entropy values, along with a comparative analysis against other recently published methodologies, including reference [26] proposing the encryption of 2D images through a multiple-order optical transform based on chaos, reference [16] introducing a pioneering algorithm for encrypting color images utilizing iterative mixing of color channels in conjunction with chaos, [42] the focus is exclusively on the estimation of parameters derived from symbolic sequences produced by a chaotic system are displayed in Tables 7 and 8. With the entropy values closely approaching 8, it is evident that the suggested algorithm is highly effective, yielding a substantial level of disturbance.

Table 7. The entropy of both the original and encrypted images.

Image	Channels	Image original	Encrypted image
4.1.02	**Red**	6.2498844	7.99831036
	Green	5.9641513	7.99877970
	Blue	5.9309190	7.99909711
	Average	6.0483183	7.99872906
4.1.04	**Red**	7.2548728	7.99906030
	Green	7.2703826	7.99885938
	Blue	6.7825005	7.99910950
	Average	7.1025853	7.99900973
4.2.05	**Red**	6.4310516	7.9990407
	Green	6.5389311	7.9986954
	Blue	6.2320377	7.9989805
	Average	6.4006735	7.9989055
4.2.03	**Red**	7.7066718	7.9998850
	Green	7.47443158	7.99852283
	Blue	7.7522171	7.99910689
	Average	7.64444020	7.9991716
4.2.07	**Red**	7.37196642	7.9996310
	Green	7.64164954	7.9993211
	Blue	7.1730455	7.9988355
	Average	7.39555383	7.9992625

Table 8. The entropy comparison results of our method.

Encrypted image	Channels	Our	Entropy		
			Kaur *et al.* [25]	**Faragallah *et al.* [16]**	**Wu *et al.* [43]**
Lena	**Red**	7.9991052	–	7.7771	–
	Green	7.9988110	–	7.7190	–
	Blue	7.9986068	–	7.7150	–
	Average	7.9988410	7.9938	7.73703	7.9973
Baboon	**Red**	7.9998850	–	–	–
	Green	7.9985228	–	–	–
	Blue	7.9991068	–	–	–
	Average	7.9991716	7.9852	–	7.9989
Peppers	**Red**	7.9996310	–	–	–
	Green	7.9993211	–	–	–
	Blue	7.9988355	–	–	–
	Average	7.9992625	7.9956	–	–

6. Conclusions

In this scholarly article, a novel encryption technology is meticulously investigated. This innovative approach constitutes a skillful hybrid technique that synergistically integrates the salient attributes of chaotic maps and group-based transformations. The recent scientific advancement in encryption owes its genesis to the development of more adept keys, deftly leveraging chaotic maps, and the introduction of a novel image transformation methodology based on the principles of group theory. As a result of these advancements, we have attained the capability to skillfully convolve neighboring pixels within an image, ingeniously devising a robust scrambling scheme by orchestrating the random reorientation of their positions. This meticulous process effectively eradicates any semblance or linkages to the source image, ensuring a high degree of encryption.

A comprehensive array of evaluation criteria is judiciously employed, encompassing meticulous entropy analysis, precise histogram examination, meticulous coefficient of correlation assessments, which encompass both neighboring pixels and the plain and encrypted image, along with the scrupulous examination of NPCR and UACI differential attacks. Each criterion is subject to a meticulous and in-depth analysis. Consequently, it becomes evident that the proposed strategy presents a highly promising and effective approach to encrypt images, thereby bolstering their security and safeguarding sensitive information from prying eyes.

References

[1] Arroyo D., Rhouma R., Alvarez G., Li S., and Fernandez V., "On the Security of a New Image Encryption Scheme Based on Chaotic Map Lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 3, pp. 033112, 2008. https://doi.org/10.1063/1.2959102

[2] Belazi A., Hermassi H., Rhouma R., and Belghith S., "Algebraic Analysis of a RGB Image Encryption Algorithm Based on DNA Encoding and Chaotic Map," *Nonlinear Dynamics*, vol. 76, no. 4, pp. 1989-2004, 2014. DOI:10.1007/s11071-014-1263-y

[3] Borujeni S. and Eshghi M., "Chaotic Image Encryption System Using Phase-Magnitude Transformation and Pixel Substitution," *Telecommunication Systems*, vol. 52, pp. 525-537, 2013. DOI: 10.1007/s11235-011-9458-8

[4] Cong L., Xiaofu W., and Songgeng S., "A General Efficient Method for Chaotic Signal Estimationin," *IEEE Transactions on Signal Processing*, vol. 47, no. 5, pp. 1424-1428, 1999. DOI: 10.1109/78.757236.

[5] Elazzaby F., El Akkad N., and Kabbaj S., "A New Encryption Approach Based on Four-Square and Zigzag Encryption (C4CZ)," *in Proceedings of the Embedded Systems and Artificial Intelligence*, Fez, pp. 589-597, 2019. https://doi.org/10.1007/978-981-15-0947-6_56

[6] Elazzaby F., El Akkad N., and Kabbaj S., "Advanced Encryption of Image Based on S-Box and Chaos 2D (LSMCL)," *in Proceedings of the 1st International Conference on Innovative Research in Applied Science, Engineering and Technology*, Meknes, pp. 1-7, 2020. DOI:10.1109/IRASET48871.2020.9092254

[7] Elazzaby F., EL Akkad N., Sabour K., and Kabbaj S., "An RGB Image Encryption Algorithm Based on Clifford Attractors with a Bilinear Transformation," *in Proceedings of the 5th International Conference on Big Data and Internet of Things*, Rabat, pp. 116-127, 2021. https://doi.org/10.1007/978-3-031-07969-6_9

[8] Elazzaby F., EL Akkad N., Sabour K., and Kabbaj S., "A New Contribution of Image Encryption Based on Chaotic Maps and the Z/nZ Group," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 1, pp. 37-47, 2023. https://www.researchgate.net/publication/367546427

[9] Elazzaby F., EL Akkad N., Sabour K., and Kabbaj S., "A New Encryption Scheme for RGB Color Images by Coupling 4D Chaotic Laser Systems and the Heisenberg Group," *Multimedia Tools and Applications*, pp. 1-20, 2023. https://doi.org/10.1007/s11042-023-16139-6

[10] El Akkad N., Merras M., Saaidi A., and Satori., K., "Camera Self-Calibration with Varying Parameters from two Views," *WSEAS Transactions on Information Science and Applications*, vol. 10, no. 11, pp. 356-367, 2013. https://www.wseas.org/multimedia/journals/information/2013/e045705-255.pdf

[11] Es-Sabry M., El Akkad N., Merras M., Saaidi A. and Satori K., "A Novel Text Encryption Algorithm Based on the Two-Square Cipher and Caesar Cipher," *in Proceedings of the 3rd International Conference of Big Data, Cloud and Applications*, Kenitra, pp. 78-88, 2018. https://doi.org/10.1007/978-3-319-96292-4_7

[12] Es-sabry M., El akkad N., Merras M., Saaidi A., and Satori K., "A New Image Encryption Algorithm Using Random Numbers Generation of two Matrices and Bit-Shift Operators," *Soft Computing*, vol. 24, pp. 3829-3848, 2020. https://doi.org/10.1007/s00500-019 04151-8

[13] Es-sabry M., El akkad N., Merras M., Saaidi A., Satori K., "A New Color Image Encryption Using Random Numbers Generation and Linear Functions," *in Proceedings of the Embedded Systems and Artificial Intelligence*, Fez, pp. 581-

588, 2019. https://doi.org/10.1007/978-981-15-0947-6_55

[14] Es-Sabry M., El Akkad N., Merras M., Saaidi A., and Satori K., "Grayscale Image Encryption Using Shift Bits Operations," *in Proceedings of the International Conference on Intelligent Systems and Computer Vision*, Fez, pp. 1-7, 2018. DOI:10.1109/ISACV.2018.8354028

[15] Essaid M., Akharraz I., Saaidi A., Mouhib A., Mohamed E., Ismail A., Abderrahim S., and Ali M., "A New Color Image Encryption Algorithm Based on Iterative Mixing of Color Channels and Chaos," *Advances in Science, Technology and Engineering Systems Journal*, vol. 2, no. 5, pp. 94-99, 2017. DOI:10.25046/aj020515

[16] Faragallah O., Alzain M., El-Sayed H., Al-Amri J., El-Shafai W., Afifi A., Naeem E., and Soh B., "Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding," *IEEE Access*, vol. 7, pp. 4184-4194, 2019. DOI:10.1109/ACCESS.2018.2879857

[17] Gray R., *Entropy and Information Theory*, Springer Science and Business Media, 2011. https://doi.org/10.1007/978-1-4419-7970-4

[18] Guo H., Zhang X., Zhao X., Yu H., and Zhang L., "Quadratic Function Chaotic System and its Application on Digital Image Encryption," *IEEE Access*, vol. 8, pp. 55540-55549, 2020. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9040448

[19] Hilborn R., *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*, Oxford University Press, 2001.

[20] Hua Z., Zhou Y., Pun C., and Chen C., "2D Sine Logistic Modulation Map for Image Encryption," *Information Sciences*, vol. 297, pp. 80-94, 2015. https://doi.org/10.1016/j.ins.2014.11.018

[21] Hua Z. and Zhou Y., "One-Dimensional Nonlinear Model for Producing Chaos," *EEE Transactions on Circuits and Systems-I: Regular Papers*, vol. 65, no. 1, pp. 235-246, 2018. DOI:10.1109/TCSI.2017.2717943

[22] Hua Z., Zhou Y., and Huang H., "Cosine-Transform-Based Chaotic System for Image Encryption," *Information Sciences*, vol. 480, pp. 403-419, 2019. https://doi.org/10.1016/j.ins.2018.12.048

[23] Jafar I., Darabkh K., and Jubair F., "Separable High Capacity Reversible Data Hiding Algorithm for Encrypted Images," *The International Arab Journal of Information Technology*, vol. 19, no. 5, pp. 812-821, 2022. https://doi.org/10.34028/iajit/19/5/13

[24] Khan J. and Ahmad J., "Chaos Based Efficient Selective Image Encryption," *Multidimensional Systems and Signal Processing*, vol. 30, pp. 943-961, 2019. https://doi.org/10.1007/s11045-018-0589-x

[25] Kaur G., Agarwal R., and Patidar V., "Multiple Image Encryption with Fractional Hartley Transform and Robust Chaotic Mapping," *in Proceedings of the 6th International Conference on Signal Processing and Integrated Networks*, Noida, pp. 399-403, 2019. DOI:10.1109/SPIN.2019.8711777

[26] Kaur G., Agarwal R., and Patidar V., "Chaos Based Multiple Order Optical Transform for 2D Image Encryption," *Engineering Science and Technology an International Journal*, vol. 23, no. 5, pp. 998-1014, 2020. https://doi.org/10.1016/j.jestch.2020.02.007

[27] Lesne A., "Chaos in Biology," *Biology Forum/Rivista di* Biologia, vol. 99, no. 3, pp. 467-481, 2006.

[28] Liu C. and Lu J., "A Novel Fractional-Order Hyperchaotic System and its Circuit Realization," *International Journal of Modern Physics B*, vol. 24, no. 10, pp. 1299-1307, 2010. https://doi.org/10.1142/S0217979210053707

[29] Lu L., Luan L., Meng L., and Li C., "Study on Spatiotemporal Chaos Tracking Synchronization of a Class of Complex Network," *Nonlinear Dynamic*, vol. 70, pp. 89-95, 2012. https://doi.org/10.1007/s11071-012-0432-0

[30] Mansouri A. and Wang X., "Image Encryption Using Shuffled Arnold Map and Multiple Values Manipulations," *The Visual Computer*, vol. 37, no. 6, pp. 189-200, 2021. DOI:10.1007/s00371-020-01791-y

[31] Mollaeefar M., Sharif A., and Nazari M., "A Novel Encryption Scheme for Colored Image Based on High Level Chaotic Maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607-629, 2017. DOI:10.1007/s11042-015-3064-9

[32] Norouzi B., Seyedzadeh S., Mirzakuchaki S., and Mosavi M., "A Novel Image Encryption Based on Hash Function with only Two-Round Diffusion Process," *Multimedia Systems*, vol. 20, pp. 45-64, 2014. https://doi.org/10.1007/s00530-013-0314-4

[33] Paschalakis S. and Lee P., "Double Precision Floating-Point Arithmetic on FPGAs," *in Proceedings of the IEEE International Conference on Field-Programmable Technology*, Tokyo, pp. 352-358, 2003. DOI:10.1109/FPT.2003.1275775

[34] Patidar V., Pareek N., and Sud K., "A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056-3075, 2009. https://doi.org/10.1016/j.cnsns.2008.11.005

[35] Skrobek A., "Cryptanalysis of Chaotic Stream Cipher," *Physics Letters A*, vol. 363, no. 1-2, pp. 84-90, 2007. https://doi.org/10.1016/j.physleta.2006.10.081

[36] Talhaoui M., Wang X., and Midoun M., "A New One-Dimensional Cosine Polynomial Chaotic Map and its Use in Image Encryption," *The Visual Computer*, vol. 37, pp. 541-551, 2020. https://doi.org/10.1007/s00371-020-01822-8

[37] Tong X., Wang Z., Zhang M., Liu Y., Xu H., and Ma J., "An Image Encryption Algorithm Based on the Perturbed High-Dimensional Chaotic Map," Nonlinear Dynamics, vol. 80, pp. 1493-1508, 2015. https://doi.org/10.1007/s11071-015-1957-9

[38] Tong X., Cui M., and Wang Z., "A New Feedback Image Encryption Scheme Based on Perturbation with Dynamical Compound Chaotic Sequence Cipher Generator," *Optics Communications*, vol. 282, no. 14, pp. 2722-2728, 2009. https://doi.org/10.1016/j.optcom.2009.03.075

[39] Wang X. and Guo K., "A New Image Alternate Encryption Algorithm Based on Chaotic Map," *Nonlinear Dynamics*, vol. 76, pp. 1943-1950, 2014. https://doi.org/10.1007/s11071-014-1259-7

[40] Wang X., Feng L., Li R., and Zhang F., "A Fast Image Encryption Algorithm Based on Non-Adjacent Dynamically Coupled Map Lattice Model," *Nonlinear Dynamics*, vol. 95, pp. 797-2824, 2019. https://doi.org/10.1007/s11071-018-4723-y

[41] Weidenmüller H. and Mitchell G., "Random Matrices and Chaos in Nuclear Physics Nuclear Structure," *Review of Modern Physics*, vol. 81, no. 2, pp. 539-589, 2009. DOI:10.1103/REVMODPHYS.81.539

[42] Wu X., Hu H., and Zhang B., "Parameter Estimation only from the Symbolic Sequences Generated by Chaos System," *Chaos Solitons Fractals*, vol. 22, no. 2, pp. 359-366, 2004. https://doi.org/10.1016/j.chaos.2004.02.008

[43] Wu X., Zhu B., Hu Y., and Ran Y., "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps," *IEEE Access*, vol. 5, pp. 6429-6436, 2017. DOI:10.1109/ACCESS.2017.2692043

[44] Wu Y., Noonan J., and Agaian S., "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. https://fliphtml5.com/vbho/fepe/basic

[45] Zhu C., "A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences," *Optics Communications*, vol. 285, no. 1, pp. 29-37, 2012. https:// doi.org/10.1016/j.optcom.2011.08.079

[46] Zhu H., Zhang X., Yu H., Zhao C., and Zhu Z., "An Image Encryption Algorithm Based on Compound Homogeneous Hyper-Chaotic System," *Nonlinear Dynamics*, vol. 89, pp. 61-79, 2017. https://doi.org/10.1007/s11071-017-3436-y

Fouzia Elazzaby she is a PhD student since 2017. She is currently a professor of computer science at the Office of Vocational Training and Employment Promotion of Fez, Morocco. She is a member of the Partial Differential Equations, Spectral Algebra and Geometry laboratories. My research interests include Cryptography, Artificial Intelligence, Image Processing.

Nabil Elakkad received the PhD degree from SMBA-Fez University in 2014. He is currently a professor of computer science at the National School of Applied Sciences (ENSA) of Fez, Sidi Mohammed Ben Abdellah University, Fez, Morocco. He is a member of the LISA and LIIAN Laboratories. His research interests include Cryptography, Artificial Intelligence, Image Processing, Data Mining, Camera Self-Calibration, 3D Reconstruction, Machine Learning, Pattern Recognition, Data Classification and Segmentation.

Khalid Sabour obtained his doctorate in the faculty of science Ibn Tofail, in 2019. He is currently a qualified mathematics teacher in Fez, Morocco. He is a member of the Partial Differential Equations, Spectral Algebra, and Geometry Laboratories. His research interests include Cryptography, Functional Analysis, Mathematical Analysis, Operator Theory, and Harmonic Analysis.