STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **12**, November 2024, pp 1956–1972.
Published online in International Academic Press (www.IAPress.org)

Utilizing the Discrete Heisenberg Group and Laser Systems in RGB Image Encryption

Fouzia El Azzaby [1,*], Khalid Sabour [1], Nabil EL AKKAD [2], Bouchta Zouhairi [3], Samir Kabbaj[1]

[1]*Department of Mathematics, Faculty of Sciences,Ibn Tofail University, KENITRA, Morocco*
[2]*Laboratory of Engineering, Systems and Applications, ENSA of Fez, Sidi Mohamed Ben Abdellah University of Fez, Morocco*
[3] *Laboratoire de Physique du Solide, Faculté des Sciences Dhar El Mahraz, Université Sidi Mohamed Ben Abdellah, B.P. 1796, Atlas, Fès 30000, Morocco*

Abstract This study signifies the endpoint of thorough cryptographic experimentation, leading to the creation of an innovative color image encryption scheme. It embodies a fusion of mathematical concepts rooted in both group theory and chaos theory. The novel encryption procedure entails the creation of cube faces, to depict the relative positions of pixels within a given stream, thereby generating six distinct channels. Within our algorithm, each monochromatic layer of an image is independently encrypted using digraph encryption. This involves a technique of rotating the four faces, followed by another rotation to encrypt the second digraph. Subsequently, matrices derived from Heisenberg theory are integrated with the monochromatic layer from the preceding step to fine-tune the image's parameters and introduce blur. Impressively, our approach has yielded promising outcomes across various images and evaluation criteria, demonstrating resilience against differential attacks and statistical analyses. Furthermore, comparative evaluations have highlighted the superiority of our method over existing algorithms.

Keywords Encryption, Laser Systems,Security, Discrete Heisenberg Group

DOI: 10.19139/soic-2310-5070-1744

1. Introduction

As social networks increasingly host a wealth of multimedia content, ensuring security has become a pressing priority to safeguard the privacy of users and organizations against potential illicit intrusions. Images, in particular, are susceptible to falling into the wrong hands, highlighting the critical importance of preserving their confidentiality. This has prompted a concerted effort among security researchers to develop robust encryption techniques tailored specifically for images, despite the plethora of existing algorithms documented in the literature ([25]-[37]). Researchers faced a significant challenge in achieving encryption comparable to that of text ([10]-[12]), as traditional methods proved inadequate due to the distinctive features of images, including their size,repetition of information, and stronger correlations. Consequently, the field of cryptography has witnessed a shift towards novel encryption methodologies, including those grounded in chaos theory ([1]-[7]), quantum theory, DNA coding, and optical systems. This shift can be attributed to the exceptional properties of chaos theory, such as determinism, sensitivity to initial conditions, and ergodicity, making it particularly attractive in recent years, especially in the realm of high-dimensional chaotic maps.
Chaotic systems can be generally classified into two categories: low-dimensional chaotic maps and high-dimensional chaotic maps. Low-dimensional maps are characterized by their simple structure and minimal number

*Correspondence to: Fouzia El Azzaby (Email: fouzia-099@hotmail.com). Department of Mathematics, Faculty of Sciences,Ibn Tofail University, KENITRA, 14000, Morocco.

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

of variables, making them predictable and vulnerable to exploitation. Conversely, high-dimensional maps boast complex structures that render them highly resistant to analysis and manipulation, thereby enhancing their suitability for cryptographic applications. Consequently, researchers have increasingly focused on harnessing the robustness of chaotic systems in cryptography, with high-dimensional chaotic maps emerging as a favored choice. For instance, Hua et al. ([14], [15]) introduced a two-dimensional sine chaotification system (2D-SCS) in 2019, aimed at increasing the complexity and expanding the chaotic ranges of 2D chaotic maps. By applying 2D-SCS to two existing chaotic maps, they demonstrated the creation of enhanced maps with significantly larger and more robust chaotic behaviors. They also detailed the development of a microcontroller-based platform for implementing these maps in hardware and explored their application in designing a pseudorandom number generator. In 2020, they introduced a two-dimensional modular chaotification system (2D-MCS) to further enhance the complexity of 2D chaotic maps, addressing observed limitations such as discontinuous chaotic ranges and incomplete output distributions. Through the bounded modular operation, 2D-MCS enabled chaotic behaviors over wide parameter ranges.Similarly, Wang et al. ([13]) developed a novel chaotic image encryption algorithm that integrates pseudo-random bit sequences and DNA planes. They utilized a coupled map lattice (CML) to design a pseudo-random bit sequence generation (PBSG) system, essential for generating the required random sequence during encryption. Initial values and parameters were determined using the SHA-256 hash algorithm along with designated keys. The image was segmented into four DNA planes according to encoding rules, followed by row and column circular permutations, and diffusion operations. Mollaeefar and Al ([18]) introduces a color image encryption method based on advanced chaotic maps (”Cosinus-Arcsinus” and ”Sinus-Power Logistic”). It involves pixel shuffling and diffusion phases, featuring an efficient permutation method tailored to the image, ensuring lower correlation and uniform color histograms for resistance against attacks. Borgia et al. ([9]) implemented a new one-dimensional chaotic map for real-time image encryption, confirmed chaotic and ergodic through theoretical analysis. Its cryptographic strength is validated using NIST statistical tests. Additionally, we propose an image encryption scheme employing two such maps for confusion and diffusion, showcasing strong cryptographic performance, while Talhaoui et al. ([16]) proposed a novel one-dimensional cosine fractional chaotic map (1-DCF) with robust cryptographic properties validated through chaos-theory analysis. Utilizing 1-DCF, we devise a rapid image encryption scheme featuring a permutation-less architecture for enhanced speed, alongside secure substitution and randomized encryption order for heightened security.

Inspired by recent advancements in encryption methodologies and driven by the shortcomings inherent in current techniques, we embarked on a journey to pioneer a novel encryption scheme. This innovative approach is rooted in the intricate dynamics of the Heisenberg group and the utilization of 4D chaotic maps. Our algorithm harnesses the inherent chaos embedded within the 4D chaotic laser system, exploiting its unpredictability to generate sequences imbued with randomness. This foundational randomness forms the cornerstone for the creation of four distinct boxes and the establishment of two critical Heisenberg matrices. Through this intricate interplay of mathematical constructs and chaotic dynamics, our encryption scheme stands poised at the forefront of cryptographic innovation. It not only addresses the deficiencies encountered in traditional encryption methods but also represents a paradigm shift towards robust and secure data protection. By marrying the complexities of modern mathematics with the chaotic nature of dynamical systems, our approach offers a promising avenue for safeguarding sensitive information in an increasingly digitized world. These elements are integral to the permutation phase of image pixels, wherein each pixel pair is encrypted by references in diagonal boxes, deepening the encryption’s robustness. Furthermore, the multiplication of image planes by Heisenberg matrices adds an additional layer of security.

Our algorithm’s effectiveness and robustness were rigorously tested against various attacks and compared favorably with existing approaches documented in the literature, affirming its viability as a potent encryption solution. Our research is structured to provide a comprehensive understanding of the study’s key aspects. We begin by elucidating the mathematical instruments utilized in the innovative framework in Section 2, supported by illustrative examples to enhance comprehension. Following this, Section 3 offers an in-depth explanation of our innovative encryption scheme, which is derived from the intricate dynamics of a four-dimensional chaotic laser system. Section 4 evaluates the experimental results, showcasing the robustness of our algorithm through a detailed examination based on various criteria and a diverse array of images. In Section 5, we conduct a comparative analysis, positioning

our technique against alternative approaches and highlighting its distinct advantages. Finally, Section 6 concludes with a summary of our findings and their implications, encapsulating the study's key insights and contributions.

2. The Mathematical Instruments Utilized in the Innovative Framework

2.1. 4D chaotic laser system

The given system represents a 4D chaotic laser system defined by a set of ordinary differential equations (ODEs). Let's break down the system:

The state variables are x_1, x_2, x_3, and x_4, representing different aspects of the laser system.

The parameters s, d, r, and b are constants that determine the behavior of the system.

The equations governing the dynamics of the system are as follows:

$$\begin{aligned}\dot{x}_1 &= s(y_1 - x_1)\\ \dot{x}_2 &= rx_1 - x_2 - x_1x_3\\ \dot{x}_3 &= x_1x_2 - bx_3\\ \dot{x}_4 &= d(x_1 - x_4)\end{aligned}$$

The system of differential equations is given by:

$$\begin{aligned}\frac{dx_1}{dt} &= s(x_2 - x_1)\\ \frac{dx_2}{dt} &= -x_2 - dx_3 + (r - x_4)x_1\\ \frac{dx_3}{dt} &= dx_2 - x_3\\ \frac{dx_4}{dt} &= -bx_4 + x_1x_2\end{aligned}$$

Here's a brief explanation of each equation:

- The first equation represents the rate of change of x_1, which depends on the difference between x_2 and x_1 multiplied by the parameter s.

- The second equation represents the rate of change of x_2, which depends on the current value of x_2, x_3, x_4, and x_1, as well as the parameters d and r.

- The third equation represents the rate of change of x_3, which depends on the current values of x_2 and x_3, and the parameter d.

- The fourth equation represents the rate of change of x_4, which depends on the current values of x_1, x_2, and the parameter b, as well as their product. The behavior of this 4D chaotic laser system can be analyzed by studying the solutions of these differential equations, often through numerical simulation techniques. Parameters s, d, r, and b can be varied to explore different regimes of behavior, including chaotic dynamics.Figure 1 represents the Behavior of x1 under different regimes.

2.2. the Heisenberg group

The Heisenberg group is a fundamental concept in mathematics, particularly in the study of Lie groups and quantum mechanics. It's named after Werner Heisenberg, one of the pioneers of quantum mechanics. The Heisenberg group, denoted as $\mathrm{H}(n)$ or $\mathrm{H}_n(\mathbb{R})$, is a specific type of non-abelian group that arises naturally in various mathematical contexts.

The Heisenberg group can be defined in several equivalent ways ([42], [43]), but one common representation is as the set of $n \times n$ upper-triangular matrices with real entries and 1's along the diagonal, and with the additional constraint that the entries above the diagonal are also real. Formally, the Heisenberg group $\mathrm{H}(n)$ consists of matrices of the form:

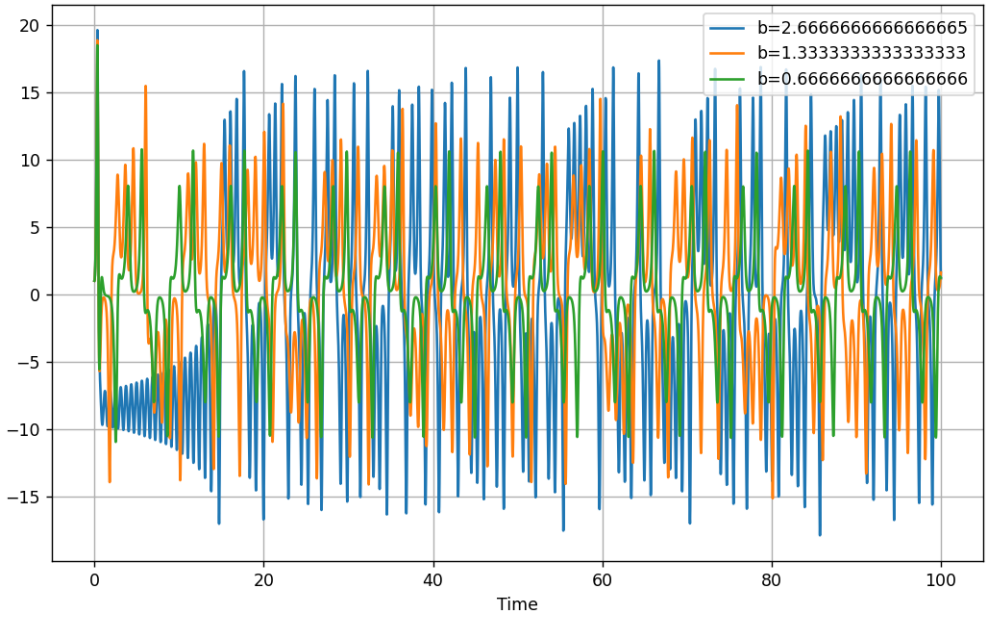


Figure 1. Behavior of x1 under different regimes.

$$A = \begin{pmatrix} 1 & x_1 & x_2 & \cdots & x_{n-1} \\ 0 & 1 & y_1 & \cdots & y_{n-2} \\ 0 & 0 & 1 & \cdots & y_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

where $x_i, y_i \in \mathbb{R}$.

The Heisenberg group exhibits intriguing properties, particularly in the context of symplectic geometry, representation theory, and harmonic analysis. It serves as a fundamental example of a non-commutative group and has applications in quantum mechanics, signal processing, and cryptography.

One classical example where the Heisenberg group naturally appears is in the study of the Schrödinger equation in quantum mechanics. The canonical commutation relation between position and momentum operators gives rise to a Lie algebra isomorphic to the Lie algebra of the Heisenberg group. This connection between the Heisenberg group and quantum mechanics is foundational in understanding the uncertainty principle, which states that certain pairs of physical properties, like position and momentum, cannot be simultaneously measured precisely.

The identity matrix serves as the neutral element in the Heisenberg group, while inverses are determined by

$$A^{-1} = \begin{pmatrix} 1 & -x_1 & x_1y_1 - x_2 & \cdots & (-1)^{n-1}x_{n-2}y_{n-2} - x_{n-1} \\ 0 & 1 & -y_1 & \cdots & (-1)^{n-2}y_{n-3} \\ 0 & 0 & 1 & \cdots & (-1)^{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

3. Proposed methodology

The technique we propose is grounded in the four-dimensional chaotic system and is implemented in two distinct phases:Phase one enables the substitution of pixels utilizing the facets of a cube, constructed using four-dimensional

maps. The second phase, we help blur the image through the coupling of prior results involving the Heisenberg group. For the purpose of image encryption, you must first encrypt each extracted plane of the three color channels (red, green, and blue) and merge them to provide us with an encrypted RGB image. Figure 6 represents the flowchart of the proposed scheme.

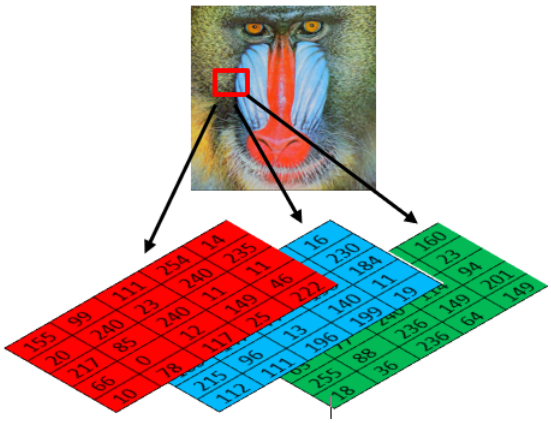


Figure 2. The retrieval of numerical values from the three planes of a basic image

Upon receiving an original RGB image designated for encryption, We partition this image into three distinct monochromatic components. Subsequently, we proceed to extract the matrix of each color, containing numerical values between 0 to 255, as illustrated in Figure 2

Subsequently, a sequence is generated through the utilization of system (S) as illustrated in Figure 3. It is based on the principles outlined in the Lorenz-Haken equations. This system features three balances and two quadratic nonlinearities. Extensive research has thoroughly explored the intricate dynamics of the chaotic regions within this 4D system, as detailed in [17].

Moreover, we trim four one-dimensional chaotic streams of magnitude 1, denoted as $(E_i)_{0\leq i\leq 3}$, from the previously generated four-dimensional sequence, where $E_0 = \{X_0, X_1, X_2, \ldots, X_n\}$, $E_1 = \{Y_0, Y_1, Y_2, \ldots, Y_n\}$, $E_2 = \{Z_0, Z_1, Z_2, \ldots, Z_n\}$, $E_3 = \{T_0, T_1, T_2, \ldots, T_n\}$, $E_4 = \{X_0 \otimes Y_0, X_1 \otimes Y_1, X_2 \otimes Y_2, \ldots, X_n \otimes Y_n\}$, and $E_5 = \{Z_0 \otimes T_0, Z_1 \otimes T_1, Z_2 \otimes T_2, \ldots, Z_n \otimes T_n\}$, with $\mathbf{n} = \{0, 1, 2, \ldots, N\}$.

Then we try to build six faces of a cube based on these streams in which each face is a 16×16 whose values are the order of each pixel to similar pixels in the same stream that gives us six random channels E'_0, E'_1, E'_2, E'_3, E'_4 and E'_5 .

Following the population of the six facets of the cube (E0′, E1′, E2′, E3′, E4′, and E5′), and the subsequent extraction of the three planes housing numerical values corresponding to the colors red, green, and blue, respectively, the process of diagraphic encryption commences. This encryption technique involves the replacement of pairs of pixels (digrams) by another pair, with each substitution being influenced by four facets. The red monochromatic plane uses the faces E0′, E1′, E5′, E3′. The green monochromatic plane uses the faces E1′, E2′, E3′, E4′, whereas the blue monochromatic plane uses the faces E0′, E4′, E5′, E2′. See Fig. 4.

We shall immediately begin the encryption procedure. Let $N \in \mathbb{N}^\star$.

Let $I = (I_{ij})_{\substack{0\leq i\leq N-1 \\ 0\leq j\leq N-1}} \in M_{N\times N}\left(\{0, 1, 2, \ldots 255\}^3\right)$, $I \in \{I_R, I_G, I_B\}$

Consider the application defined by

$\varphi : \quad \{0, 1, 2, \ldots, 255\}^3 \longrightarrow \left\{\{0, 1, 2, \ldots, 255\}^4\right\}^3$

$(I_R(i,j), I_G(i,j), I_B(i,j)) \longmapsto \varphi(X)$, where $\varphi(X) = \left(\ I'_R \quad , I'_G \quad , I'_B \ \right)$

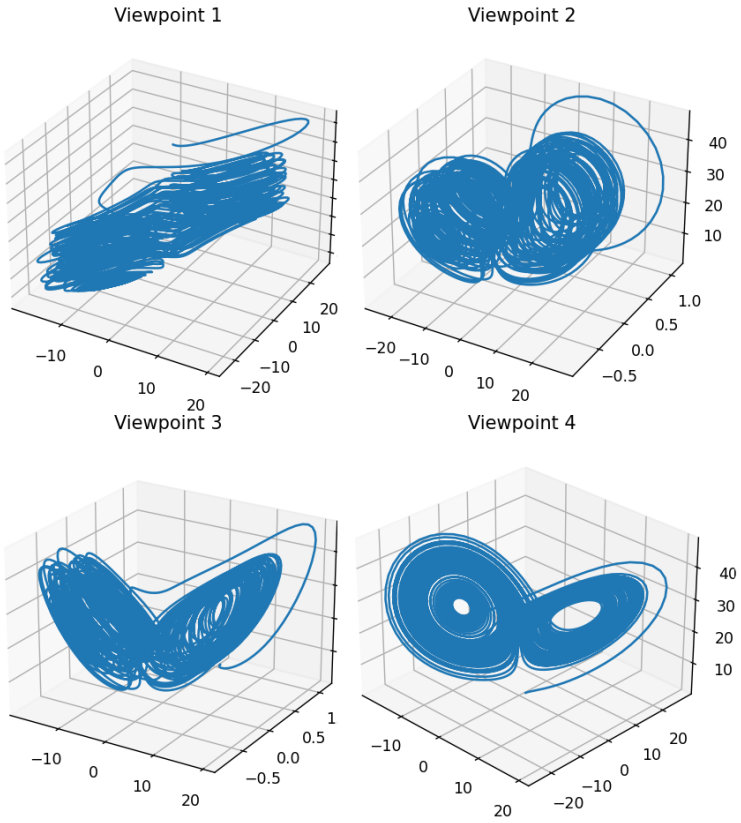


Figure 3. Plot the chaotic attractor from different orientations s = 10, d = 0.1, r = 28, b = 8/3 and with the initial values (1.0, 1.0, 1.0, 1.0)

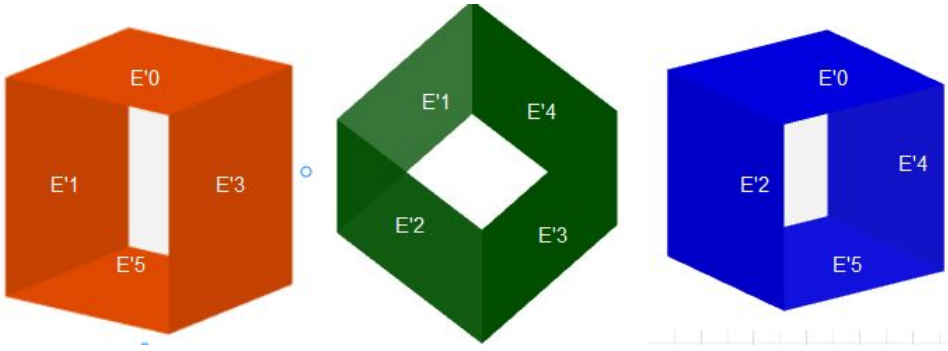


Figure 4. Faces of the cube generated by 4D chaotic laser system.

f(X) is the permutation of pixels by cube faces; for example, we can extract the digraph (A, B). from the red monochromatic of the color image and we looked the first value A in the face E'_0 and the value B in the faceE'_3 then we looked for their perpondicular in the faces E'_1 and E'_5 so that the digraph (A, B) is crypted by (A′,B′). This process is repeated with each couple of the image to be encrypted with a circular rotation of the faces i.e. for cipher the second couple we seeked the first value in the E'_1 face and the second value in the E'_0 face with this we overcome the fact that a pixel is encrypted with the same value so that our Technique is not vulnerable to

differential attacks see fig 5 . For the confusion part, we employ three Heisenberg matrices whose input parameters

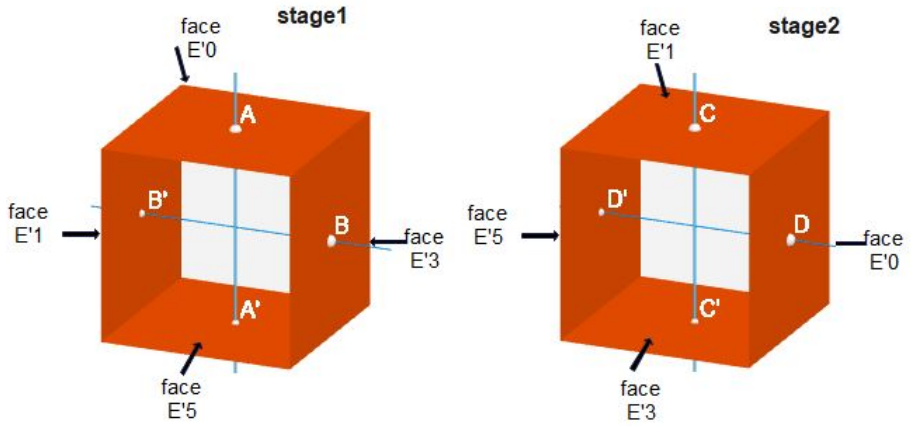


Figure 5. Example of digraph encryption process.

are calculated by the formulas below the horizontal and vertical parameters, and then we perform an ordinary product between each Heisenberg matrix and each channel from the preceding step (I'r, I'g and I'b).

$$I_R^{'} = (a_{ij})_{\substack{0\le i\le N-1\\ 0\le j\le N-1}} \qquad I_G^{'} = (b_{ij})_{\substack{0\le i\le N-1\\ 0\le j\le N-1}} \qquad I_B^{'} = (c_{ij})_{\substack{0\le i\le N-1\\ 0\le j\le N-1}}$$

$$x_i = \sum_{j=1}^{n-1} a_{ji} \quad ; x_i' = \sum_{j=1}^{n-1} b_{ji} \quad ; x_i'' = \sum_{j=1}^{n-1} c_{ji}$$

$$y_i = \sum_{j=1}^{n-1} aij \quad ; y_i' = \sum_{j=1}^{n-1} b_{ij} \quad ; y_i'' = \sum_{j=1}^{n-1} c_{ij}$$

$$z = \sum_{i=0}^{n}\sum_{j=0}^{n} a_{ij} \quad ; z' = \sum_{i=0}^{n}\sum_{j=0}^{n} b_{ij} \quad ; z'' = \sum_{i=0}^{n}\sum_{j=0}^{n} c_{ij}$$

$$H_1 := \left\{ \begin{pmatrix} 1 & x_1 & x_2 & \dots & x_n & z \\ 0 & 1 & 0 & \dots & 0 & y_1 \\ 0 & 0 & 1 & \dots & 0 & y_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & y_n \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \right\} H_2 := \left\{ \begin{pmatrix} 1 & x_1^{'} & x_2^{'} & \dots & x_n^{'} & z^{'} \\ 0 & 1 & 0 & \dots & 0 & y_1^{'} \\ 0 & 0 & 1 & \dots & 0 & y_2^{'} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & y_n^{'} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \right\}$$

$$H_3 := \left\{ \begin{pmatrix} 1 & x_1^{''} & x_2^{''} & \dots & x_n^{''} & z^{''} \\ 0 & 1 & 0 & \dots & 0 & y_1^{''} \\ 0 & 0 & 1 & \dots & 0 & y_2^{''} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & y_n^{''} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \right\}$$

For $n = 1$, the Heisenberg group H_{2n+1} is the Heisenberg group of order 3, denoted H_3. This group consists of 3×3 matrices whose entries are integers and whose determinant is equal to 1.

The definition of H_3 is as follows:

$$H_3 = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_{11} \right\}$$

To illustrate this, here is an example of such a matrix in H_3 with $n = 1$:

$$A = \begin{pmatrix} 1 & 3 & 8 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

We can also compute the inverse of this matrix in H_3. The inverse of a matrix in H_3 can be found by undoing the effect of the matrix on the basis vectors. In this case, the inverse of A would be:

$$A^{-1} = \begin{pmatrix} 1 & -3 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Here is an example of 3 x 3

$$\begin{matrix} \text{Heisenberg matrix} \end{matrix} \quad \begin{matrix} \text{Red channel} \end{matrix}$$
$$\begin{pmatrix} 1 & 3 & 8 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 50 & 150 & 200 \\ 100 & 175 & 225 \\ 75 & 125 & 250 \end{pmatrix} = \begin{pmatrix} 950 & 1675 & 2875 \\ 250 & 425 & 725 \\ 75 & 125 & 250 \end{pmatrix}$$

After applying modulo 256 to the result to ensure values between 0 and 255:

$$\begin{pmatrix} 950 & 1675 & 22875 \\ 250 & 425 & 725 \\ 75 & 125 & 250 \end{pmatrix} = \begin{pmatrix} 182 & 139 & 59 \\ 250 & 169 & 213 \\ 75 & 125 & 250 \end{pmatrix} \text{ mod } [256]$$

For decryption

Step1

To find the inverse of the Heisenberg matrix:

$$\begin{pmatrix} 1 & 3 & 8 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

We can use the fact that it is an upper triangular matrix. The inverse of an upper triangular matrix with 1s on the diagonal is also an upper triangular matrix, and its elements can be computed systematically. The inverse A^{-1} is:

$$A^{-1} = \begin{pmatrix} 1 & -3 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A^{-1} == \begin{pmatrix} 1 & -3 & -2 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 182 & 139 & 59 \\ 250 & 169 & 213 \\ 75 & 125 & 250 \end{pmatrix}$$

$$AB = A \cdot B = \begin{pmatrix} -718 & -618 & -1080 \\ 100 & -81 & -287 \\ 75 & 125 & 250 \end{pmatrix}$$

$$AB \mod 256 = \begin{pmatrix} -718 \mod 256 & -618 \mod 256 & -1080 \mod 256 \\ 100 \mod 256 & -81 \mod 256 & -287 \mod 256 \\ 75 \mod 256 & 125 \mod 256 & 250 \mod 256 \end{pmatrix} = \begin{pmatrix} 50 & 150 & 200 \\ 100 & 175 & 225 \\ 75 & 125 & 250 \end{pmatrix}$$

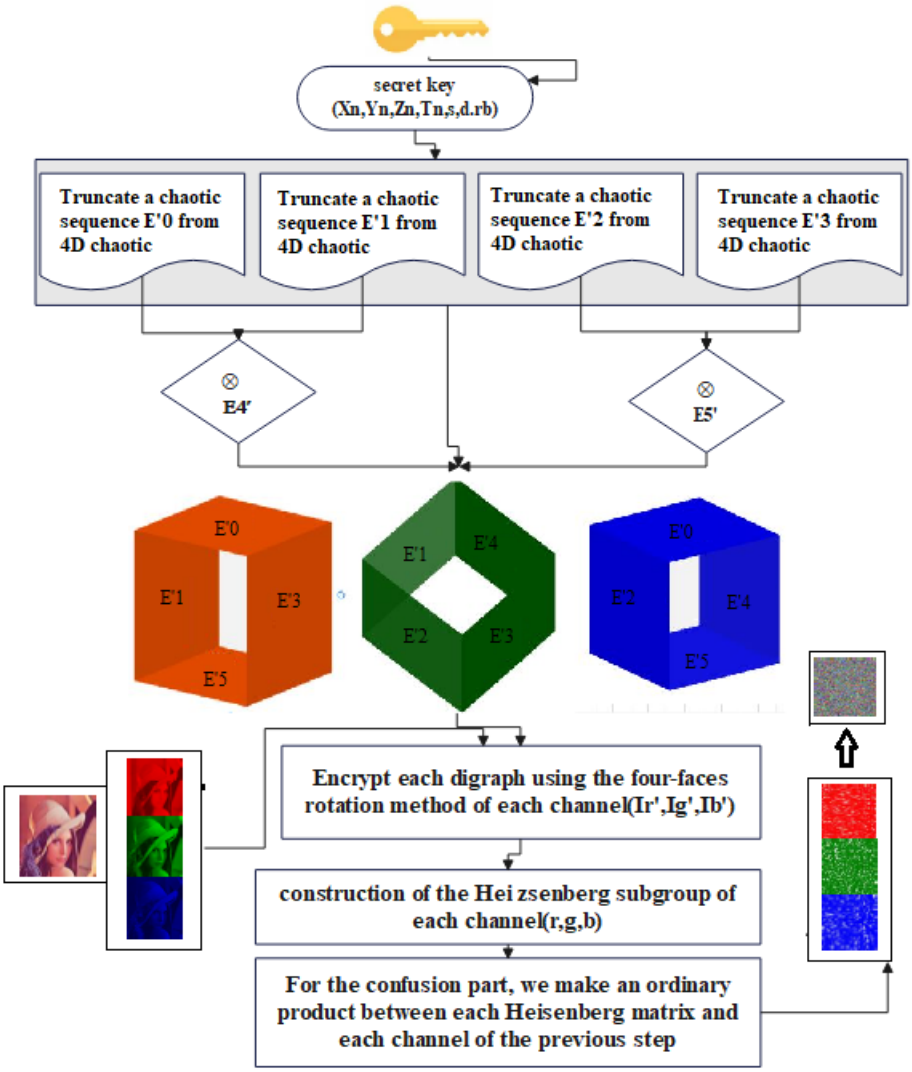


Figure 6. Proposed scheme flowchart.

4. Outcomes of the simulation

In the computational setup facilitated by the Intel® Core™ i5 processor and 4GB of RAM, Python is employed, we present some experimental results that show the robustness of the new scheme proposed against different attacks. We employed various common test images . These images were chosen as typical examples to evaluate both the effectiveness and robustness of our encryption schema.

4.1. Examination of histograms

Examining image histograms yields insights into the arrangement of luminous and shadowy tones across a picture. This methodology is frequently employed in statistical analysis, with the objective of comprehending the correlation between pixel values in the original image and those in the encrypted rendition.

Consequently, adept high-security image encryption methods strive to achieve histograms characterized by uniform distribution and minimal deviation. In Figure 7, histograms depicting various images are showcased both

before and after the encryption process. Evaluation of these histograms demonstrates that our encryption technique consistently produces encrypted images with a steady dispersion of pixel intensity values.

4.2. Analysis of Differential Attacks

Two additional metrics serve to quantify the disparity between the plain image and its encrypted equivalent: the Normalized Cross-Correlation Peak Ratio (NCPR) and the Unified Average Changing Intensity (UACI).

Attackers employ a strategy of introducing subtle modifications to the original image and subsequently applying algorithms both prior to and following encryption. This method is commonly referred to as a differential attack. The utilization of these metrics, namely NCPR and UACI, Allows for the assessment of the effectiveness and resilience of the encryption scheme against such threats. The calculation of these metrics involves the following formulas:

$$NPCR_{R,G,B} = \sum_{i,j} \frac{D_{R,G,B}(i,j)}{L} \times 100\%$$

$$UACI_{R,G,B} = \frac{1}{L}[\sum_{L,S} \frac{C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)}{255}] \times 100\%$$

where L signifies the total pixel count within the image. $C_{R,G,B}$ and $C'_{R,G,B}$ represent the ciphered images prior to and following alteration of a single pixel in the original image. $D_{R,G,B}(i,j)$ can be defined as:

$$D_{R,G,B}(i,j) = \begin{cases} 1, & \text{if } C_{R,G,B}(i,j) \neq C'_{R,G,B}(i,j) \\ 0, & \text{if } C_{R,G,B}(i,j) = C'_{R,G,B}(i,j) \end{cases}$$

Table 3 displays the outcomes yielded by our innovative schema. The NPCR surpasses 99%, while the UACI exceeds33%. These findings indicate that even the slightest alteration can result in encrypted images distinct from the originals.

Table 3. Examination of differential attack techniques

Images	NPCR	UACI
Lena	99.73749592807	33.619598908896
Baboon	99.7369867494	33.60597205966
Peppers	99.7354593235	33.619257488817
Barbara	99.7532790254	33.45930525938
House	99.74767862059	33.6186285435

4.3. Correlation between adjacent images

Correlation is a method that measures the linear relational force between two adjacent pixels. Regarding our investigation, we scrutinized the horizontal, vertical and diagonal correlations of the following original images: Lena, baboon, peppers, barabara and house. And their encrypted counterparts, generated using 5000 randomly selected data points, as illustrated in Figure 8 .

Table 4 showcases the correlation attained across vertical, horizontal, and diagonal orientations. The obtained results substantiate that the novel approach adeptly removes such correlation.

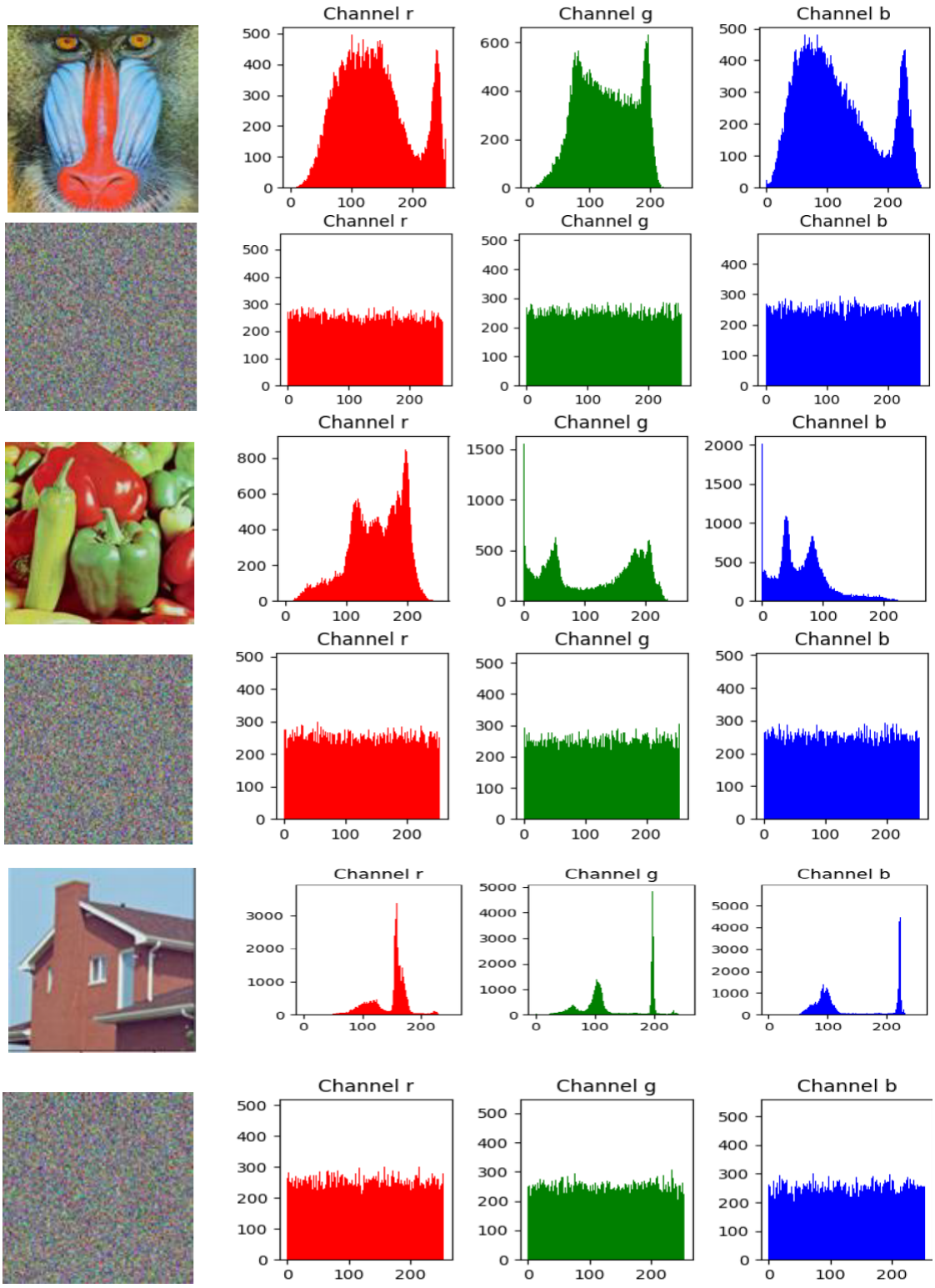
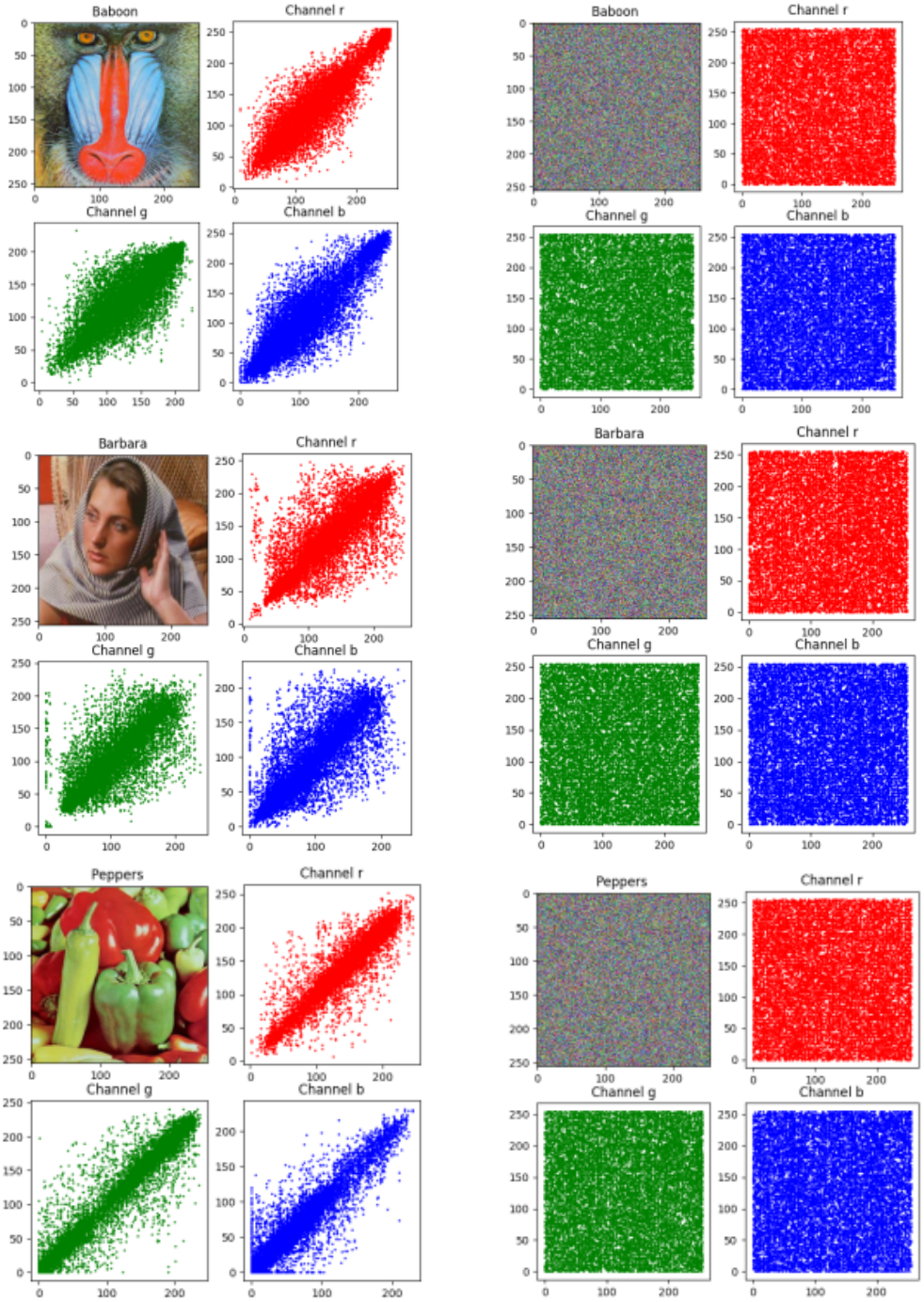


Figure 7. Histograms of the original red, green, and blue (R, G, B) images alongside the corresponding encrypted R, G, B images


Baboon
Channel r
Channel g
Channel b
Barbara
Channel r
Channel g
Channel b
Peppers
Channel r
Channel g
Channel b
Baboon
Channel r
Channel g
Channel b
Barbara
Channel r
Channel g
Channel b
Peppers
Channel r
Channel g
Channel b

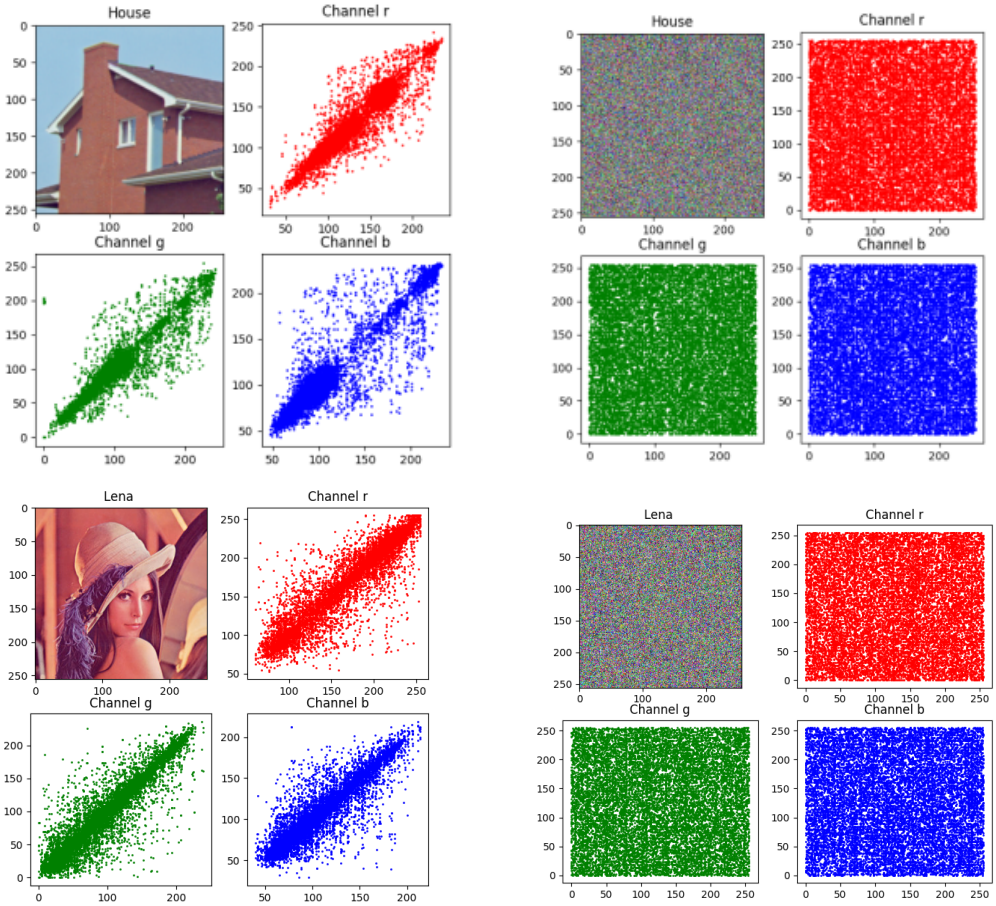


Figure 8. Distributions of correlation among neighboring pixels in both plain and encrypted images.

Table 4.Sustained Correlation Between Plain and Cipher Images

images	Direction	Original image				Encrypted image			
		Red	Green	Blue	Avg	Red	Green	Blue	Avg
Baboon	Horizontal	0.935087	0.885568	0.924876	0.914786	-0.001184	-0.014931	0.023684	0.002524
	Vertical	0.904731	0.832747	0.904727	0.881200	-0.011277	-0.002772	0.015974	0.000640
	Diagonal	0.882861	0.794286	0.879732	0.853132	0.016770	-0.001813	0.010517	0.008477
Barbara	Horizontal	0.809452	0.779951	0.805354	0.797218	-0.008680	-0.001891	-0.007268	-0.005959
	Vertical	0.936451	0.927722	0.942773	0.929075	0.008930	0.025835	0.017278	0.017343
	Diagonal	0.745966	0.707481	0.749950	0.732816	0.015533	0.025276	-0.020579	0.006781
Peppers	Horizontal	0.938212	0.963273	0.934292	0.945101	-0.000687	0.026436	-0.016112	0.003239
	Vertical	0.944010	0.967306	0.940356	0.950321	-0.009329	-0.003706	-0.001819	-0.004959
	Diagonal	0.903727	0.944581	0.902125	0.917455	-0.001146	0.006243	0.013479	0.006187
House	Horizontal	0.958729	0.970816	0.972331	0.967312	-0.006118	0.003224	-0.009870	-0.004252
	Vertical	0.926505	0.932339	0.965273	0.941408	0.008021	-0.021643	0.005073	-0.002858
	Diagonal	0.905135	0.916732	0.949664	0.921409	-0.015983	0.018171	0.027989	0.010062
Lena	Horizontal	0.936611	0.932883	0.909192	0.925725	0.018657	-0.024656	0.010700	0.001561
	Vertical	0.963106	0.956293	0.936855	0.952476	0.008210	0.016019	0.014612	0.012939
	Diagonal	0.912781	0.904831	0.877108	0.898677	-0.005794	-0.040163	-0.001074	-0.015665

4.4. Analysis of information entropy

The entropy proposed by Shannon aims to evaluate the unpredictability and non-deterministic characteristics of the information inherent in the generated encrypted images. Emphasizing the significance, it's noted that 8 persists as the optimal theoretical value for information entropy to mitigate against statistical attacks. The calculation follows thusly:

$$H(C) = -\sum_{i=0}^{255} p\left(C_i\right) \log_2 p\left(C_i\right)$$

In this context, $p(C_i)$ represents the probability associated with encountering pixel value intensity i within image C. Table 5 illustrates the entropy metrics of images cryptographically processed using our approach. The resulting data validates that our proposed method consistently attains a substantial level of entropy across most encrypted images.

Table 5.Analysis of entropy

images	lena	baboon	peppeer	barhaxa	house
entrope	7.998001	7.997713	7.997801	7.995671	7.997256

5. Comparative examination

To validate the effectiveness of our novel encryption approach in the exploration of chaotic systems and their correlation with the principles of the Heisenberg matrix, We performed an extensive comparison with cutting-edge methodologies referenced as [22], [40], [19], [20], [41], [39], [38], [8], [21], [23], and [24]. This experiment was designed to encompass various criteria, including UACI,NPCR,entropy and correlation coefficient.

Table 6. The NPCR and UACI outcomes obtained from the Lena image encrypted by our method and those of the literature

scheme	NPCR	UACI
Ref.[38]	99.6071	33.4692
Ref.[39]	99.60679	33.3741
Ref.[8]	99.5693	33.4386
Ref.[23]	99.56	31.17
Ref.[5]	99.63785	33.58601
Our	99.73749	33.61959

Table 6 exhibits the outcomes regarding UACI and NPCR achieved by our encryption methodology when compared to encryption schemes outlined in recent literature, specifically referenced in [38], [39],[5], [8], and [23]. These results indicate that our technique is fully capable of rivaling the latest advancements documented in the literature.

Table7. Result of entropy comparison between our algorithm and an alternative approach

image	Our	Ref.[5]	Ref.[22]	Ref.[40]	Ref.[19]	Ref.[41]
lena	7.998001	7.997428	7.9938	7.737033	7.613966	7.5863

Table 7 contains the entropy outcomes for the encrypted Lena image, juxtaposed with algorithms referenced as [40], [22], [41], and [19]. Notably, the entropy value closely approaches 8, which is widely regarded as the ideal benchmark according to established literature. This proximity to the ideal value underscores the

robustness of our algorithm in safeguarding confidentiality against potential unauthorized attacks.

Table 8.Correlation coefficient comparison pertaining to the Lena image

Schema	channel			
	red	green	blue	average
Ref.[40]	−0.000066	0.0367	0.0247	0.020444
Ref.[21]	0.0074	- 0.0031	- 0.0021	0.000733
Ref.[24]	0.0085	0.0127	-0.0155	0.0019
Ref.[33]	0.007621	0.005257	-0.007645	0.001744
Ref.[20]	0.1204	0.0985	0.1002	0.106366
Ref.[5]	0. 0070923	- 0.01643133	0.008171	-0.000389
Our	0. 001561	0.012939	-0.015665	-0.0003883

Table 8 illustrates the comparative analysis of correlation coefficient values among our newly devised encryption methodology and the algorithms elucidated in the cited references [40], [21], [5],[24], [20], and [33], specifically for the Lena image. Notably, our algorithm yields correlation coefficients that approach zero, aligning closely with the results derived from sophisticated schemes. This significant deviation from resemblance ensures that there is minimal similarity discernible between the original single-color image and its encrypted counterpart.

6. Conclusion

This study signifies the culmination of comprehensive investigative efforts aimed at developing an innovative framework for encrypting color images within the domain of data security. The methodology is rooted in systems of differential equations, characterized by three equilibria and two quadratic non-linearities, integrating principles from the discrete Heisenberg matrix. At the outset, pseudo-random numbers are generated to amplify the intricacy of the chaotique system's output. Subsequently, four streams are truncated to yield six facets, each comprising unique integers spanning from 0 to 255. These facets coalesce into 16-by-16 matrices, encoding the spatial arrangements of pixels within their respective streams, thus yielding six distinct channels.

Subsequently, our cryptographic procedure proceeds to independently encrypt each monochromatic layer of the provided image.The encryption procedure commences, utilizing the six previously generated facets through digram encryption, followed by a circular rotation of the four facets. During the diffusion phase, a standard product computation takes place between the monochromatic layer obtained from the preceding encryption stage and the matrices derived from the Heisenberg group.

The empirical findings underscore the resilience of our approach against a spectrum of attacks, encompassing differentials, statistical analyses, and contemporary algorithms elucidated in recent literature.

Conflict of interest

The authors declare that they have no competing interests.

REFERENCES

1. Elazzaby, F. EL akkad, N., kabbaj, S, *Advanced encryption of image based on S-box and chaos 2D(LSMCL)*, 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). 2020.
2. Elazzaby, F., El Akkad, N., Kabbaj, S. *A New Encryption Approach Based on Four-Square and Zigzag Encryption (C4CZ)*, Embedded Systems and Artificial Intelligence (Springer). 1076, 589-597(2020).
3. Elazzaby, F. EL akkad, N., Sabour, KH., kabbaj, S., *An RGB Image Encryption Algorithm Based on Clifford Attractors with a Bilinear Transformation,* International Conference On Big Data and Internet of Things (Springer), 2022, .vol. 489 , 116-127.
4. Elazzaby F., elakkad 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.
5. Elazzaby F., EL akkad N., Sabour KH. and kabbaj S., *A new encryption scheme for RGB color images by coupling 4D chaotic laser systems and the Heisenberg group,* Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-16139-6.

6. Elazzaby F., EL akkad N., Sabour KH., *The Coupling of a Multiplicative Group and the Theory of Chaos in the Encryptions of Images,* The International Arab Journal of Information Technology, Vol. 21, No. 1, January 2024
7. ElAzzaby, F., Sabour, K.H., ELakkad, N., El-Shafai, W., Torki, A., Rajkumar,S.R., *Color image encryption using a Zigzag Transformation and sine–cosine maps,* Scientific African, Volume 22, 2023,
8. Talhaoui, MZ., Wang, X. Midoun, MA., Midoun,M. *A new one-dimensional cosine polynomial chaotic map and its use in image encryption*, 37, 541–551 (2021)
9. Boriga, R., Dascalescu, A.C., Diaconu, A.-V. *A new onedimensional chaotic map and its use in a novel real time image encryption scheme*, Adv. Multimed. 2014, 6 (2014)
10. Rijmen, V., Daemen, J. *Advanced encryption standard*, In: Proceedings of Federal Information Processing Standards Publications.National Institute of Standards and Technology, 19–22(2001)
11. Coppersmith, D. *The data encryption standard (DES) and its strength against attacks*, IBM J. Res. Dev. 38(3), 243–250 (1994)
12. Rivest, R.L., Shamir, A., Adleman, L. *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM 21(2), 120–126 (1978)
13. Wang, X., Zhao, H.,Hou,Y., Luo, C., Zhang,Y.,Wang, C. *Chaotic image encryption algorithm based on pseudo-random bit sequence and dna plane*, Mod. Phys. Lett. B 33(22), 1950263 (2019)
14. Hua, Z., Zhou Y., Bao, B. *Two-Dimensional Sine ChaotificationSystem With Hardware Implementation*, IEEE Transactions on In-dustrial Informatics, 16, 887-897 (2020)
15. Hua Z, Zhou Y, Huang H. *Cosine-transform-based chaotic system for image encryption*, Inf Sci 480:403–419 (2019)
16. Talhaoui, M.Z., Wang, X., Talhaoui, A. *A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme*, The Visual Computer 37, 1757–1768 (2021)
17. Natiq, H.; Said, M.R.M.; Al-Saidi, N.M.; Kilicman, A. *Dynamics and Complexity of a New 4D Chaotic Laser System*, Entropy 2019,21, 34; doi:10.3390/e21010034
18. Mollaeefar, M., Sharif, A., Nazari, M., *A novel encryption scheme for colored image based on high level chaotic maps*, Multimed. Tools Appl. 76(1), 607-629(2017).
19. Wu, X., Zhu, B., Hu, Y.,Ran, Y., *A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps*, IEEE Access 5, 6429-6436 (2017).
20. Kang, XJ., Tao, R. *Color image encryption using pixel scrambling operator and reality-preserving MPFRHT*, IEEE T Circ Syst Vid 29(7), 1919–1932 (2019).
21. Kaur, G., Agarwal, R., Patidar, V. *Multiple image encryption with fractional Hartley transform and robust chaotic mapping*, in: 6th International Conference on Signal Processing and Integrated Networks (SPIN) IEEE 399-403 (2019)
22. Kaur, G., Agarwal, R., Patidar, V. *Chaos based multiple order optical transform for 2D image encryption*, Engineering Science and Technology an International Journal, 2020.
23. jain andsharma,R., J.B. *Symmetric color image encryption algorithm using fractional DRPM and chaotic baker map*, in Proc . IEEE Int.Conf.Recent Trends Electron., INf Commun Technol.(RTEICT), 1835-1840 (2016).
24. Kumar, M., Powduri,P., Reddy, A. *An RGB image encryption using diffusion process associated with chaotic map*, J. Information Security Appl. 21, 20–30 (2015)
25. El Akkad, N., Saaidi, A., Satori, K. *Self-calibration based on a circle of the cameras having the varying in-trinsic parameters*, Proceedings of 2012 International Conference on Multimedia Computing and Systems,ICMCS. 161-166 (2012).
26. El akkad, N., Merras, M., Saaidi, A., Satori,K. *Camera self-Calibration with Varying Parameters from Two views*, Wseas Transactions on Information Science and Application, 10(11), 356-367,(2013).
27. El akkad, N., Merras, M., Saaidi, A., Satori, K. *Robust Method For Self-Calibration Of Cameras Having The Varying Intrinsic Parameters*, Journal Of Theoretical And Applied Information Technology 50(1), 57-67 (2013).
28. El akkad, N., El Hazzat, S., Saaidi, A., Satori, K. *Reconstruction of 3D Scenes by Camera Self-Calibration and Using Genetic Algorithms*, 3D Re-search, 6(7), 1-17 (2016).
29. El Akkad, N., Merras, M., Baataoui, A., Saaidi, A.,Satori, K. *Camera self-calibration having the varying parameters and based on homography of the plane at infnity*, Multimedia Tools and Applications. 77(11), 14055-14075 (2018).
30. Es-Sabry, M., El Akkad, N., Merras, M., Saaidi, A.,Satori K. *A novel text encryption algorithm based on the two-square Cipher and Caesar Cipher*, Int Conf Big Data Cloud Appl. 872, 78-88 (2018).
31. Es-sabry, M., El akkad, N., Merras, M., Saaidi, A., Satori, K. *A New Color Image Encryption Using Random Numbers Generation And Linear Functions*, Embedded Systems and Artifcial Intelligence (Springer), 581-588, (2020).
32. Es-Sabry, M., El Akkad, N., Merras, M., Saaidi,A., Satori, K. *Grayscale image encryption using shift bits operations*, International Conference on Intelligent Systems and Computer Vision. 1-7,(2018).
33. Es-sabry, M., El akkad, M., Merras, M., Saaidi, A.,Satori,K. *A Novel Color Image Encryption Approach Based On Random Numbers Generation Of Two Matrices And Bit-Shift Operators*, Soft Computing (Springer), (2019). https://doi.org/10.1007/s00500-019-04151-8.
34. Essaid,M. ,Akharraz, I., Saaidi, A., Mouhib,A.,Mohamed, E., Ismail, A., Abderrahim S., 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. 2, 94-99 (2017).
35. Merras, M., El Akkad, N., Saaidi, A., Nazih, A.G.,Satori, K. *Camera calibration with varying parameters based on improved genetic algorithm*, WSEAS Transactions on Computers. 13, 129-137, (2014).
36. Merras, M., Saaidi, A., El Akkad, N., Satori, K. *Multi-view 3D reconstruction and modeling of the unknown 3D scenes using genetic algorithms*, Soft Computing. 22(19), 6271-6289, (2018).
37. El Hazzat, S., Merras, M., El Akkad, N., Saaidi, A.,Satori, K. *Enhancement of sparse 3D reconstruction using a modified match propagation based on particle swarm optimization*, Multimedia Tools and Applications. 78(11), 14251-14276, (2019).
38. Wang, X., Feng,L., Li,R., Zhang ,F. *A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model*, Nonlinear Dyn 1-28(2019)
39. Hua, Z., Zhou, Y., Huang, H. *Cosine-transform-based chaotic system for image encryption*, Inf. Sci.480,403-419(2019)

40. Faragallah, O.S., Alzain,M.A., El-Sayed,H.S., Al-Amri, J.F., El-Shafai,W., Afifi,A., Naeem,E.A., Soh, B. *Block-based optical color image encryption based on double random phase encoding*, IEEE Access 7 (2019) 4184–4194.
41. Mishra, D.C., Sharma, R.K., Suman, S., Prasad, A. *Multi-layer security of color image based on chaotic system combined with RP2DFRFT and Arnold transform*, J. Information Security Appl., 37 (2017) 65-90.
42. Sabour, K.H., Charifi, A., Kabbaj, S. *On a Variant of μ-Wilson's Functional Equation with an Endomorphism,* In: Anastassiou, G., Rassias, J. (eds) Frontiers in Functional Equations and Analytic Inequalities. Springer, Cham. https:// doi.org/10.1007/978-3-030-28950-8_5 (2019)
43. K. Sabour, *Wilson's functional equation with an endomorphism,* Math-Recherche et Application 15 (2016), 32–39.