Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption based on Hyperchaotic System

by Edy Winarno

Submission date: 15-Jun-2023 09:51PM (UTC+0700)
Submission ID: 2116677002
File name: FINAL_Article.pdf (3.02M)
Word count: 10635
Character count: 54054

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption based on Hyperchaotic System

Edy Winarno[1], Kristiawan Nugroho[1], Prajanto Wahyu Adi[2], De Rosal Ignatius Moses Setiadi[3], Member, IEEE

[1] Faculty of Information Technology and Industry, Universitas Stikubank, Semarang, Central Java, Indonesia
[2] Faculty of Science and Mathematics, Universitas Diponegoro, Semarang, Central Java, Indonesia
[3] Faculty of Computer Science, Dian Nuswantoro University, Semarang, Central Java, Indonesia

Corresponding author: Edy Winarno (edywin@edu.unisbank.ac.id).

ABSTRACT The quality of encryption is dependent on the complexity of the confusion-diffusion pattern and the quality of the keystream employed. To enhance complexity and randomness, this study proposes a combination of multiple interleaved patterns, including Zigzag, Hilbert, and Morton patterns to complicate the confusion-diffusion. The keystream is generated from the improved logistic map and the 6D hyperchaotic map, which complement each other due to their sensitivity to initial conditions and control parameters. This produces highly random and nonlinear keystreams, making them difficult to predict. The encryption process consists of four phases, alternating between diffusion and confusion. Furthermore, SHA-512 is used to enhance key space and sensitivity. Based on the test results, the proposed encryption technique can withstand various attacks, such as statistics, differential, brute force, and NIST randomness tests, as well as data loss and noise attacks. Most of the results are better than previous studies.

INDEX TERMS 6D Hyperchaotic System; Image Encryption; Improved Logistic Map; Multi-Interleaved Encryption; Novel Confusion-Diffusion Pattern

I. INTRODUCTION

Image encryption secures images by applying cryptography techniques to prevent unauthorized access and maintain information confidentiality. In the increasingly advanced digital world, data security becomes more important, especially when the data contains confidential or important information[1]–[3]. Images are a type of data often used and shared online, making image encryption increasingly important. Images have several intrinsic characteristics, such as high redundancy, large volume, and high correlation between adjacent pixels, that must be considered when performing the encryption process.[4]–[6]. So the image encryption should be specifically designed to suit the characteristics of the image better.

Chaos-based encryption has become a popular method in image encryption due to the unique characteristics of chaos systems. The primary reasons for using chaos are its certain properties, such as apparent randomness, non-linearity, aperiodicity, ergodicity, and extreme sensitivity to initial conditions and control parameters[7]–[9]. Based on Shannon's confusion and diffusion, traditional cryptographic theory can also be associated with the intrinsic characteristics of chaotic systems, making chaotic maps a suitable choice for designing encryption systems on images[10]–[13]. In fact, from a modern cryptographic perspective, only a few of these algorithms are insecure and have been broken in cryptanalysis[14]. However, not all of the latest image encryption methods are fully analyzed and comprehensively evaluated for cryptanalysis attacks [15] [16]. Although chaotic systems offer many benefits for image encryption, the security of chaotic image encryption algorithms can be compromised due to flawed algorithm designs [17]. Then the algorithm must be designed with a comprehensive analysis of security weaknesses. In addition, it is necessary to pay attention to the one-to-one relationship between the secret key and the chaotic system parameters and adopt an iterative structure or a combination of different encryption operations[15].

Chaos-based encryption has significantly developed from more superficial complexity, such as 1-Dimensional (1-D) or 2-D chaotic systems, to higher complexity, such as hyperchaotic systems in 3-D, 4-D, 5-D, 6-D, and even 7-D.

Among the widely used 1-D chaotic systems are Logistics, Intertwining, Henon, Chebyshev, Tent maps, and so on[18], [19], while for 2-D there are Arnold and 2D logistic-sine-coupling maps[20]–[22]. Traditional hyperchaotic systems generally have 3D; the widely applied ones are Lorentz, Chen, Lu, Rossler, etc. Meanwhile, hyperchaotic systems with higher dimensions can be developed by combining or modifying several chaotic system methods. Each chaos method has unique characteristics in terms of stability, a number of fixed points, frequency and speed of convergence to the steady state level, bifurcation, and resulting fractal structure[23]–[26].

Bifurcation and Lyapunov exponent (LE) are important characteristics in designing chaotic systems. Bifurcation refers to the change in a dynamic system's orbit structure, while LE measures the system's sensitivity to initial conditions and determines its chaos level. LE values can be positive, negative, or close to zero, indicating the system's stability or instability[27], [28]. The LE values can be positive, negative, or close to zero. Negative values indicate a stable system, positive values indicate an unstable system, and values close to zero indicate the boundary between stability and instability. Stable systems can be used for encryption that is difficult to predict, while unstable systems generate encryption keys that are sensitive to initial conditions[23]–[25]. The hyperchaotic system was defined as employing at least two positive LEs, one zero LE, and the rest of is negative LEs[29]. Yang et. al [30] proposed new hyperchaotic 6D system which has four positive LE, one zero LE, and one negative LE. With most LE positives, the method's sensitivity is very high towards the initial state. So that hyperchaotic is implemented in this paper.

When implemented in the image encryption method, the excellent hyperchaotic quality must also be supported by good diffusion and confusion quality. To achieve the confusion property, the plain image pixels' positions and values are randomly altered under the supervision of a secret key. Additionally, the diffusion property is manifested by a single-pixel position alteration being capable of producing significant changes in the cipher image[20]. The previous studies attempted to improve the quality of encryption by creating combinations and variations of confusion and diffusion operations. Confusion and diffusion in image encryption are performed at least at the pixel level[31]–[33]. Still, they can also be combined at the bit-level and pixel level [5], [8], [34]–[36], usually done on row and column images. Other techniques used include bit-plane expansion both horizontally and vertically[37], cyclic shift technique[18], [38], [39], multi-directional pada column, row, and diagonal [40], [41], plane-level permutation[42], 3D bit-plane[43], etc. The diffusion and confusion methods applied to grayscale images are generally applied to RGB colour images with repetition techniques. The interleaved colour channel method can be used in encryption methods explicitly designed for colour images to improve encryption quality. This technique can mix the three channels evenly before the diffusion and confusion operations are performed. Another hypothesis that can be concluded is that combining or modifying patterns will increase the complexity and security of image encryption. Based on the literature above, this research has contributions and objectives to:

1. The design combined interleaved patterns for diffusion and confusion based on Zigzag, Hilbert, and Morton.
2. Combine a 6D hyperchaotic system and a 1D chaotic system to improve security.
3. The encryption method is designed alternately with confusion and diffusion patterns in four phases, done at the pixel and bit levels.
4. It uses dual SHA-512 hash functions to increase both keys and plaintext sensitivity.

The remaining manuscript is organized into four parts: section 2, which contains preliminaries that explain related work theoretical literature, and ideas for modifying the method. Section 3 includes a detailed explanation of the stages of the proposed method. Section 4 is Results and Analysis, which presents the dataset, test results, and analysis. Finally, section 5 is the conclusion of the objectives, results, and analysis.

II. PRELIMINARIES

A. 6D HYPERCHAOTIC SYSTEM

A hyperchaotic system is a dynamic system with random and unpredictable properties that can be used to generate secure encryption keys for digital image encryption. A hyperchaotic system must have a minimum of two positive exponents Lyapunov numbers and one zero value to ensure the diversity and complexity of its dynamics [29]. When the system parameters change to exhibit highly random behavior, a hyperchaotic system must exhibit extensive and complex bifurcations. A hyperchaotic system cannot have a stable balance point, so the system can exhibit random and unpredictable behavior.

Some popular hyperchaotic in digital image encryption are Lorenz, Chen, Lü, Rössler and Chua hyperchaotic. Initially, hyperchaotic was constructed with three to four dimensions. In its development, more recent research tries to develop hyperchaotic systems with higher dimensions to increase security and complexity in digital image encryption. As in research [44], combining 4D hyperchaotic + 2D chaotic system. Then research [45] that implements the 6D hyperchaotic system made by Grassi et al. [46] with multi-wing hyperchaotic attackers.

Recently Yang et al. [30] proposed a six-dimensional (6D) hyperchaotic system that has a hidden attractor and complex dynamics with four positive Lyapunov exponents. This hyperchaotic 6D system has unusual properties, such as the unlimited number of singularly degenerate heteroclinic cycles and the bifurcation of the singular orbit to the hidden hyperchaotic attractor, so its dynamics become very

complex. Thus, the 6D hyperchaotic will perform extraordinarily if properly applied to image encryption. Eq. (1) used to generate 6D hyperchaotic system by Yang, et al.

$$\begin{aligned} \dot{x}_1 &= h(x_2 - x_1) + x_4, \\ \dot{x}_2 &= -fx_2 - x_1x_3 + x_6, \\ \dot{x}_3 &= -l + x_1x_2, \\ \dot{x}_4 &= -x_2 - x_5, \\ \dot{x}_5 &= kx_2 + x_4, \\ \dot{x}_6 &= gx_1 + mx_2, \end{aligned} \tag{1}$$

where $h > 0, l > 0, f, k, g,$ and $m \neq 0$ are parameters. If the values of $h = 10, l = 100, f = 2, k = 7, g = -1, m = 1$, the 6D Hyperchaotic system (1) have a hidden attractor due to the absence of equilibrium, and the Lyapunov exponents will have the maximum number of positive values, which is four, along with one zero and one negative value, as $LE_1 = 1.3613$, $LE_2 = 0.0733$, $LE_3 = 0.0478$, $LE_4 = 0.0189$, $LE_5 = 0.0000$, and $LE_6 = -14.2010$.

B. LOGISTIC MAP AND ITS DEVELOPMENT

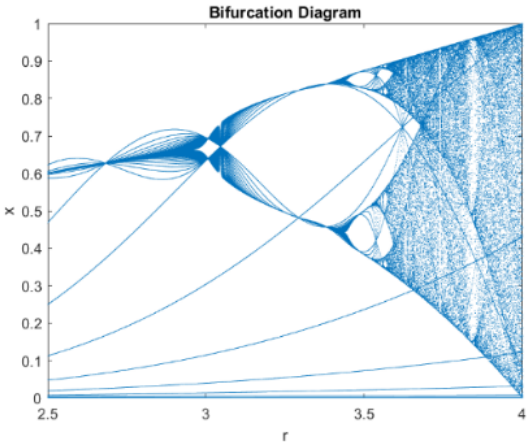
A logistic map is a mathematical equation with nonlinear iteration that can be used to generate chaotic sequences. A logistic map is simpler than a hyperchaotic system because it is only a one-dimensional chaotic system. A logistic map can be calculated using Eq. (2),

$$x_{n+1} = rx_n(1 - n) \tag{2}$$

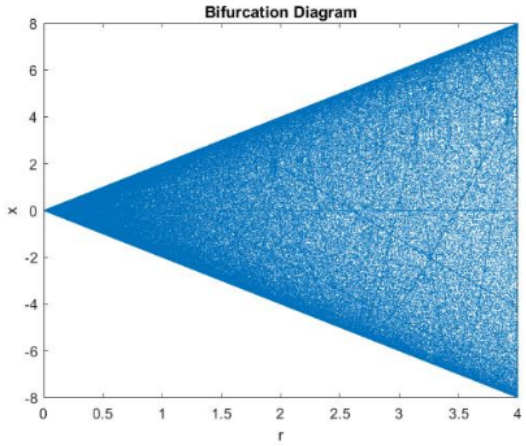
Where x_{n+1} is the value of variable x at time $n + 1$, x_n is the value of variable x at time n, r is the control parameter.

In the Logistic Map equation, the dynamic system moves towards a stable state when the growth parameter value is low. However, when the growth parameter value is increased, the dynamic system can experience bifurcation and change to a more complex state, such as periodic oscillation or chaos. Every time the growth parameter value passes through a bifurcation point, the number of peak points on the diagram doubles, indicating a sharp change in the system behavior. The higher the growth parameter value, the more complex the system behavior; the system can become highly chaotic at a certain point. Therefore, the bifurcation property in the Logistic Map equation shows that the dynamic system can experience a sharp change in its behavior when the growth parameter value exceeds certain critical values, see Fig. 4(a). This is also confirmed by the LE spectrum shown in Fig. 5(a), where there is a dynamic change in the LE value from zero, negative, and positive. Positive values indicate the tendency of the system to become chaotic, while negative values indicate the tendency of the system to converge to a fixed point. The LE value is zero, meaning the dynamic system is at a critical point between stable and chaotic behavior[47]. This makes the value of r in the Logistic Map equation greatly affect the properties of the resulting chaotic sequence.

$$x_{n+1} = 2r - r_n^2/r \tag{3}$$

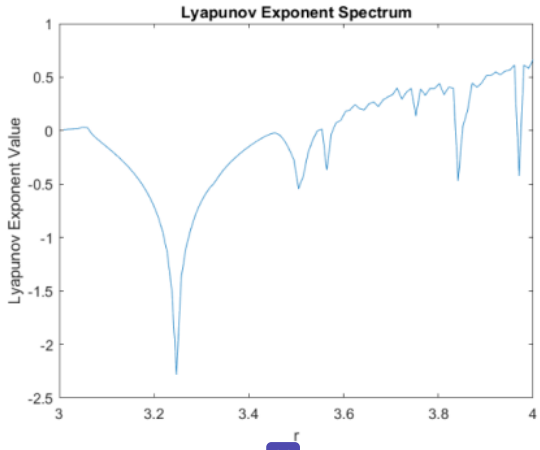


(a)

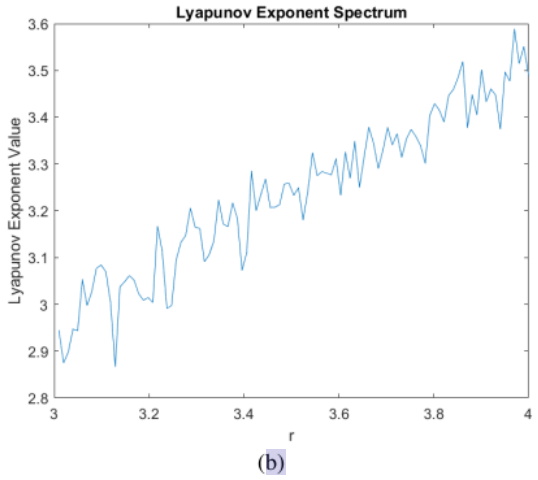


(b)

FIGURE 1. Bifurcation Diagram Plot {(a) Logistic Map; (b) Improved Logistic Map}



(a)



(b)

FIGURE 2. Lyapunov Exponent Spectrum Plot {(a) Logistic Map; (b) Improved Logistic Map}

The Logistic map was developed into the Improved Logistic map (ILM) in a research[48], where ILM can be calculated using Eq. (3). The bifurcation diagram plot of ILM in Fig. 4(b) and the Lyapunov exponent spectrum shown in Fig. 5(b) indicate chaotic phenomena and relatively constant Lyapunov exponents as the value of r changes. All LE values are positive, making the ILM highly sensitive to initial conditions and capable of increasing key variations. Note that the highest LE value in the logistic map is 0.663463317703722, while in the ILM, it is 3.588305170397140, indicating that the ILM method is designed to be more sensitive to changes in the initial value of x.

C. HASH FUNCTION

Hash functions are crucial in increasing the variation and security of keys in encryption, especially in image encryption. Hash functions are commonly used for encrypting keys, where keys of varying lengths are encrypted and transformed into a fixed-length hash value. Image encryption has been widely applied in various research, such as in [10], [11], [44], [49]–[51] to improve security, particularly in the key space. SHA-512 is a Secure Hash Algorithm (SHA) designed by the United States National Security Agency (NSA) that produces a unique 512-bit or 64-byte hash value for each different input, including files, messages, passwords, and various multimedia files such as images. The advantage of SHA-512 is its high security due to its complex and mathematically-based structure[52]. The key space of SHA-512 is 2^{512} or approximately 1.34×10^{154}, which is much larger than SHA-128 and SHA-256 with key space of 2^{128} or approximately 3.40×10^{38} and 2^{256} or approximately 1.17×10^{77}, respectively, making it resistant to brute-force attacks.

III. PROPOSED METHOD

Based on the hypotheses from various literature discussed in section 1 and section 2, this research proposes a method of color image encryption using the Yang 6D hyperchaotic system, ILM, and SHA-512 to obtain a feasible encryption system that is resistant to various attacks, sensitive to small changes in the key, and has a large keyspace. In addition, 1D interleaved, confusion and diffusion operations are applied at the pixel and bit levels, as shown in Fig. 3.

1. Read the RGB plain image as input for SHA-512, resulting in an output hash value.
2. Convert the hash value into ASCII numbers to set the initial condition (x) of ILM, and calculate x using Eq. (4).

$$x = \frac{\sigma(hash)}{div}, div \begin{cases} \sigma > 100, & div = 1000 \\ \sigma > 10, & div = 100 \\ \sigma > 1, & div = 10 \end{cases} \quad (4)$$

   Where σ is the standart deviation.
3. Generate a chaotic sequence using Eq. (3) with x as the initial condition and n as the number of pixels in the image.
4. Sort the chaotic sequence in ascending order and save the sorted index.
5. On the other side, convert the RGB plain image (input) into a linear 1D interleaved color plane array as output using Algorithm 1.

Algorithm 1: Converting color image to interleaved color plane 1D array function
Input : A color image in RGB format Output : A 1D array containing interleaved color plane pixel values
1 : m, n, channels ← size of the input image 2 : output ← an mn3 x 1 empty array to store the interleaved color plane pixel values 3 : for i = 1 to m do 4 : for j = 1 to n do 5 : output[(i-1)n3 + (j-1)*3 + 1] ← the red channel pixel value at position (i,j) of the input image 6 : output[(i-1)n3 + (j-1)*3 + 2] ← the green channel pixel value at position (i,j) of the input image 7 : output[(i-1)n3 + (j-1)*3 + 3] ← the blue channel pixel value at position (i,j) of the input image 8 : end for 9 : end for 10: return the output array

6. Perform confusion on the array with permutation operations based on the index order of the chaotic sequence. After confusion, reshape the array into an RGB matrix.
7. On the other side, input the secret key, perform the SHA-512 operation, then convert it into ASCII numbers to obtain 64 hash numbers.

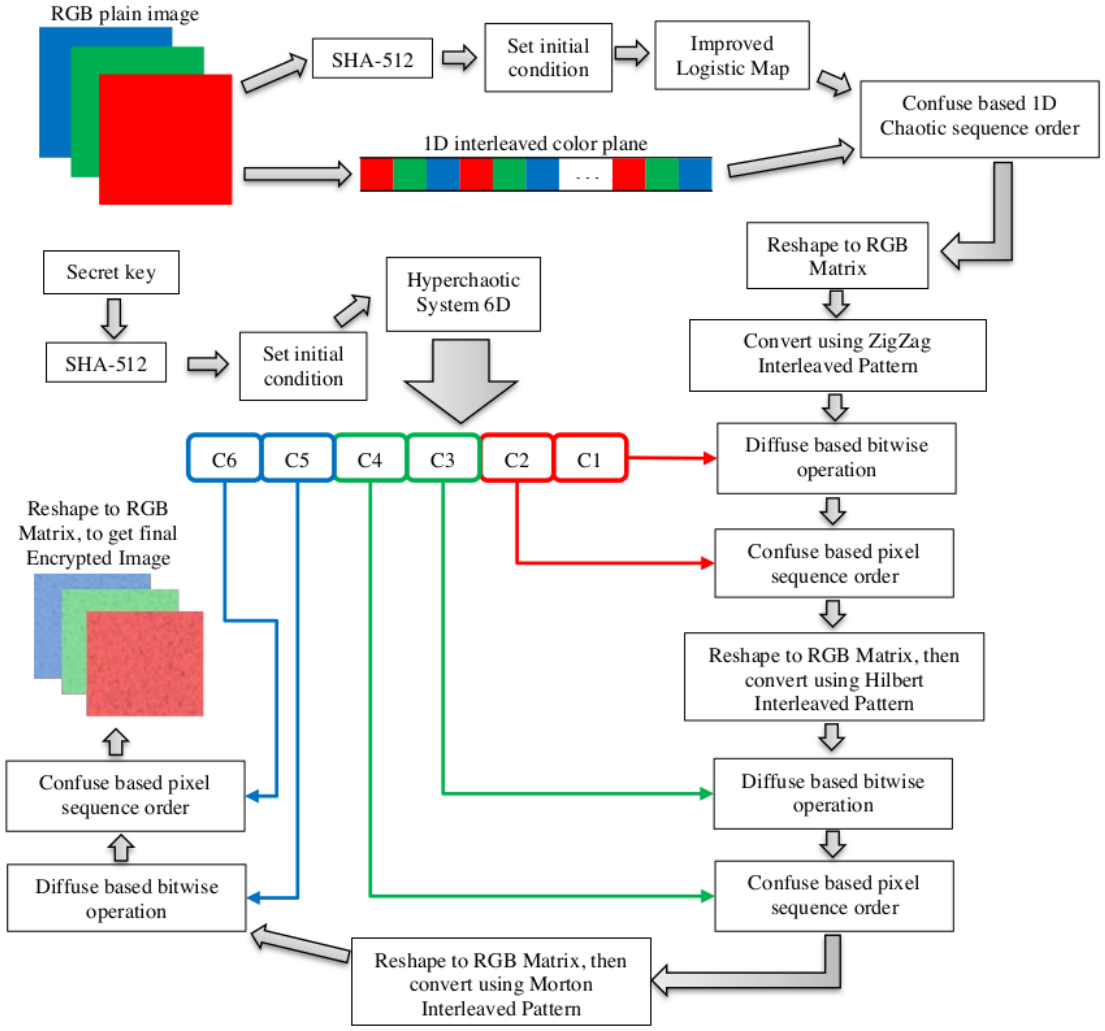


FIGURE 3. Proposed Encryption Flow

8. Calculate the initial condition (x_1, x_2, x_3, x_4, x_5, and x_6) of the enhanced 6D Hyperchaotic system using Eq. (5).

$$\begin{aligned} x_1 &= \sigma(hash[1:24]), \\ x_2 &= \sigma(hash[9:32]), \\ x_3 &= \sigma(hash[17:40]), \\ x_4 &= \sigma(hash[25:48]), \\ x_5 &= \sigma(hash[33:56]), \\ x_6 &= \sigma(hash[41:64]), \end{aligned} \tag{5}$$

9. Generate six chaotic sequences, namely $c1, c2, c3, c4, c5$, and $c6$, using Eq. (1) with x_1, x_2, x_3, x_4, x_5, and x_6 as the initial conditions, respectively.
10. The chaotic sequence is real numbers. They cannot be directly used to perform diffusion using bit-wise XOR operation. So, convert three chaotic sequences $(c1, c3, c5)$ to integer values using Eq. (6).

$$\begin{aligned} c1 &= mod(round(|c1(1:n) \times 10^9|), 256), \\ c3 &= mod(round(|c3(1:n) \times 10^9|), 256), \\ c5 &= mod(round(|c5(1:n) \times 10^9|), 256), \end{aligned} \tag{6}$$

11. Convert the confused RGB matrix into the interleaved array using a zigzag scan, like Fig. 4(a). Then perform diffusion using bit-wise XOR operation with $c1$.
12. Convert the RGB matrix into the interleaved array using the Morton scan, like Fig. 4(c). Then perform diffusion using bit-wise XOR operation with $c5$.
13. Perform confusion using swap operation and sequence order of c4. After confusion, reshape the array into an RGB matrix.
14. Combine the R, G, and B color channels to obtain the encrypted image.

Based on the scheme and method stages, can be concluded that four main stages of encryption are carried out. In the first stage, linear scanning is carried out to form an interleaved array for the confusion process with swap permutations based on the chaotic sequence order. In the second, third, and fourth stages, diffusion is carried out with a bit-wise XOR operation followed by a swap operation based on a chaotic sequence order. The bit-wise operation is carried out so that diffusion is carried out at the bit-level while the confusing stage is carried out at the pixel-level, where the diffusion and confuse processes are alternated to increase the randomness. Three different interleave scan patterns are also proposed, namely Zigzag, Hilbert, and Morton, so the effects of diffusion and confusion are more scattered and complicate randomization, which impacts increasing security. More details on testing and a discussion of the results are explained in the next section.

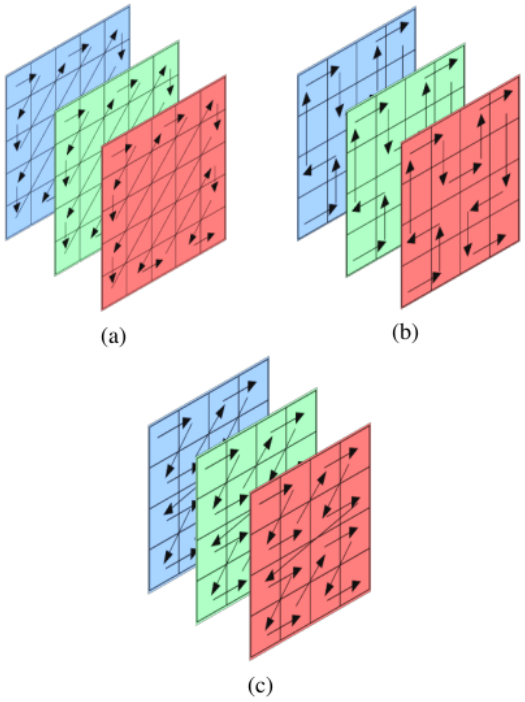


FIGURE 4. Illustration of Interleaved Pattern using {(a)Zigzag Scan; (b) Hilbert Scan; (c) Morton Scan}

IV. RESULTS AND ANALYSIS

The proposed method is tested on 24-bit color images commonly used in various studies, such as[8], [11], [18], [32], [53], [54], to facilitate the comparison process. All images are resized to have dimensions of 256 × 256. The images used are color images presented in Fig. 5. The method implementation uses the Matlab R2016a application, with hardware specifications using an i7-1165G7 @2.80GHz processor and 16GB RAM.

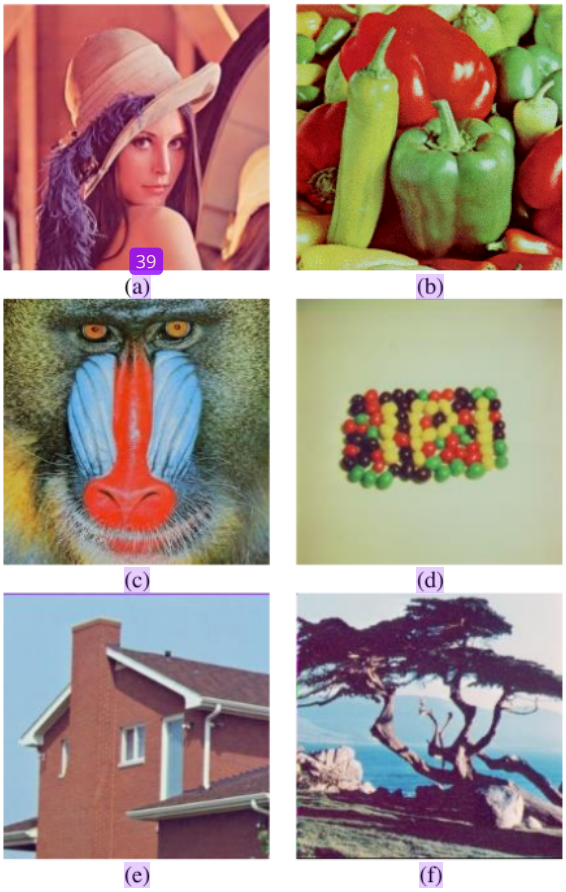
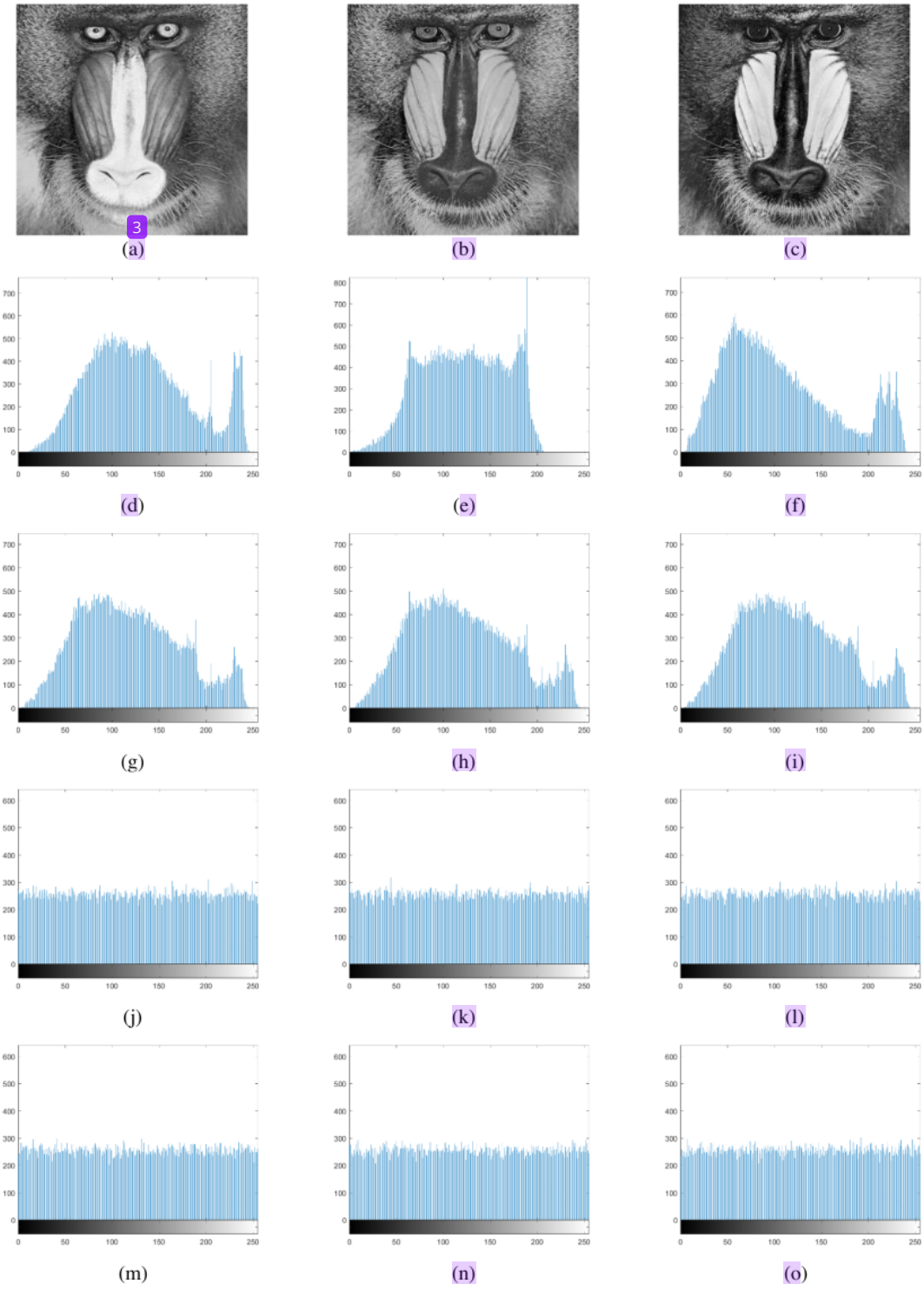


FIGURE 5. Image Dataset {(a) Lena; (b) Peppers; (c) Baboon; (d) Jelly Beans; (e) House; (f) Tree}

Fig. 6 presents the histograms of each color channel at each stage, while Table 1 briefly presents the encryption results at each stage along with their respective RGB histograms. Visually, the histogram of stage 1 or the first confusion process, appears to produce a similar pattern in each channel due to the interleaved 1D operation. In the first stage, the histogram does not appear uniform, but there is a relatively similar distribution in each channel, and there is a significant visual change in the RGB image. Histograms are one of the indicators of image encryption quality, which is responsible for visualizing the distribution spread. An excellent histogram should appear relatively uniform in each bin, indicating that the encryption results perform well. In stage 2, diffusion is performed at the bit-level, then confusion at the pixel-level, resulting in a uniform histogram where the average bin value is around 275, see Fig. 6(j-l) and Table 1 3rd row. Furthermore, in stages 3 and 4, diffusion is performed at the pixel level to increase complexity and encryption quality. The results appear more random with a more visually uniform histogram, see Fig. 6(m-o) and Table 1 (rows 4 and 5). However, further security tests are needed

to validate the proposed method's performance. The results of various security tests are presented in section IV.A to IV.H.



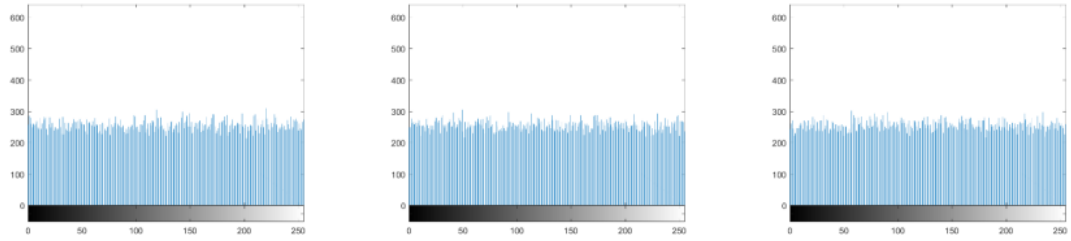
(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

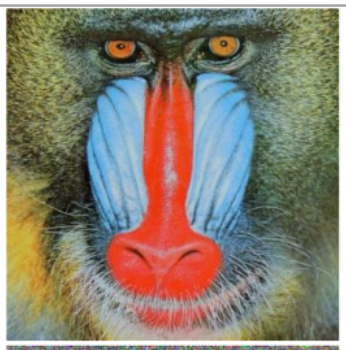
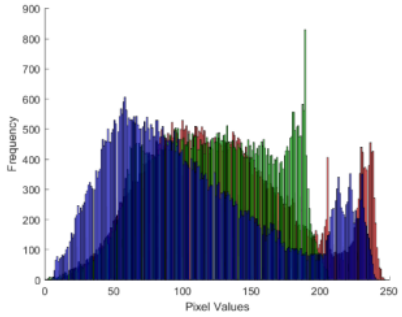
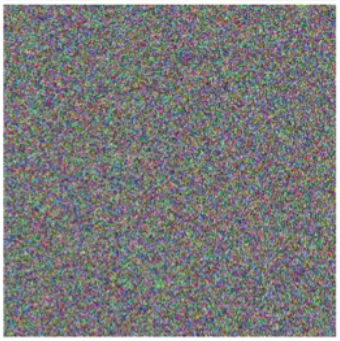
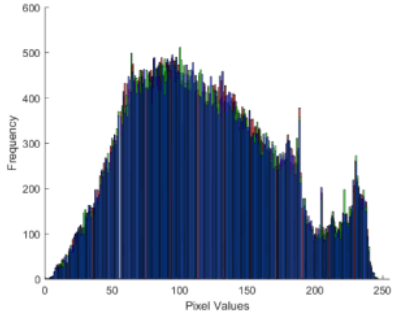
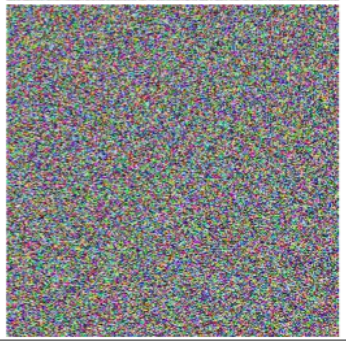
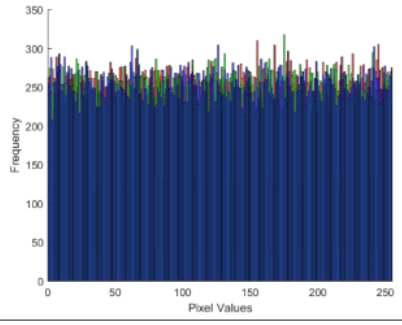
(m) (n) (o)



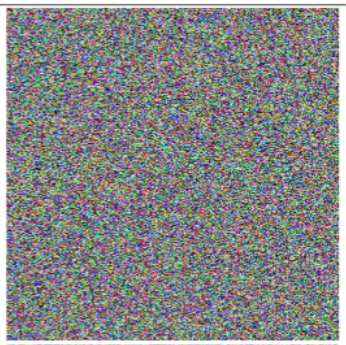
(p) (q) r)

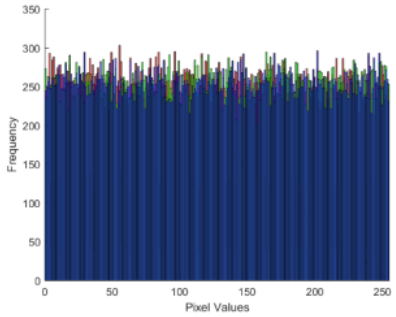
FIGURE 6. Details Histogram every channel of Sample Image Results {(a), (b),(c) Original Chanel Layer of R, G, and B, respectively; (d), (e), (f) Original Histogram of Chanel Layer R, G, and B, respectively; (g), (h), (i) After phase 1 Histogram of Chanel Layer R, G, and B, respectively; (j, (k), (l) After phase 2 Histogram of Chanel Layer R, G, and B, respectively; (m), (n), (o) After phase 3 Encrypted Histogram of Chanel Layer R, G, and B, respectively; (p),(q),(r) Final Encrypted Histogram of Chanel Layer R, G, and B, respectively}

TABLE I
SAMPLE ENCRYPTION RESULTS IN DETAILS

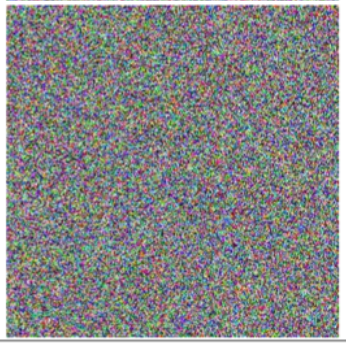
Stage	Results	Histogram
Original Image		
Stage 1 Encryption		
Stage 2 Encryption		

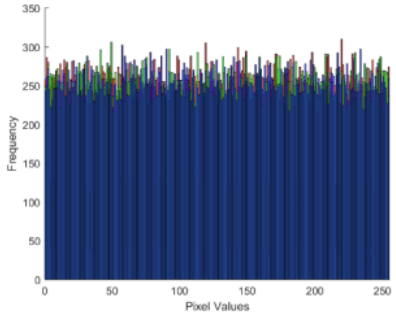
Stage 3 Encryption





Stage 4/ Final Encryption





A. CHI-SQUARE ANALYSIS

The first security test conducted is the chi-square (X^2) analysis. This test is used to confirm the uniformity of the histogram of the encrypted image and includes a test of resistance to statistical attacks on the image. With the chi-square test, numerical results are obtained to ensure that the histogram of the encrypted image is uniform. If the resulting chi-square value is smaller than or equal to $X^2_{\delta,df}$ =293.2478 with a significance level $(\delta) = 0.05$ and degrees of freedom (df) of 255, then the histogram will be confirmed to be uniform. The chi-square value can be calculated using Eq. (7).

$$X^2 = \sum_{i=1}^{256} \frac{\left(P_i - \frac{P}{255}\right)^2}{\frac{P}{255}} \quad (7)$$

Where i ranges from 1 to 256 in Matlab due to its indexing starting at 1. The grey recurrence value (P_i) refers to the value assigned to each instance of the i-th grey value. Table 2 presents the results of the chi-square measurements on the proposed method, where it can be seen that all chi-square values have passed and validated the uniformity of the histogram. Table 3 also presents a comparison of the chi-square values with previous works.

TABLE II
CHI-SQUARE RESULTS

Image	Red	Green	Blue	Passed?
Lena	213.0796	202.5793	215.3674	Yes
Baboon	225.1314	231.2321	227.2132	Yes
Peppers	220.6378	237.3112	235.2388	Yes
Jelly Beans	211.1231	229.3239	229.1314	Yes
House	242.2142	215.3213	224.2132	Yes
Tree	237.2131	234.9479	233.1213	Yes
Average	224.8999	225.1193	227.3809	Yes

TABLE III
CHI-SQUARE COMPARISON WITH THE PREVIOUS METHOD

Image	Method	Red	Green	Blue
Lena	[32]	244.4375	243.5703	243.8242
	[11]	241.1484	210.7031	267.6484
	Proposed	213.0796	202.5793	215.3674
Baboon	[11]	259.0566	273.2832	271.7031
	Proposed	225.1314	231.2321	227.2132

B. INFORMATION ENTROPY ANALYSIS

Entropy analysis is a statistical analysis technique used to understand how random or non-random a given data or signal is. In image encryption, entropy analysis can be used to determine how effective encryption is in scrambling the image. Entropy in image encryption is measured from zero to eight because an image can be considered a discrete data source with 256 possible pixel values (0-255)[55]. Therefore, if each pixel value has an equal probability, the maximum entropy is the log base 2 of 256, equivalent to eight.

$$H = \sum_{i=1}^{n} p(c_i) log_2 \left(\frac{1}{p(c_i)}\right) \quad (8)$$

Eq. (8) used to calculate entropy involves the total number of symbols (n), the information source represented by c_i, and the probability of occurrence of the source c_i represented by $p(c_i)$. The results of entropy measurements are presented in Table 4, and all values are close to eight. This suggests that

the encryption quality based on entropy is excellent. Furthermore, Table 5 shows that the proposed encryption method performs better than previous works.

TABLE VI
INFORMATION ENTROPY RESULTS

Image	Red	Green	Blue	Average RGB
Lena	7.9976	7.9978	7.9976	7.9977
Baboon	7.9977	7.9976	7.9978	7.9977
Peppers	7.9977	7.9975	7.9977	7.9976
Jelly Beans	7.9975	7.9977	7.9978	7.9977
House	7.9976	7.9977	7.9978	7.9977
Tree	7.9977	7.9978	7.9975	7.9977
Average	7.9976	7.9977	7.9977	7.9977

TABLE V
ENTROPY COMPARISON WITH THE PREVIOUS METHOD

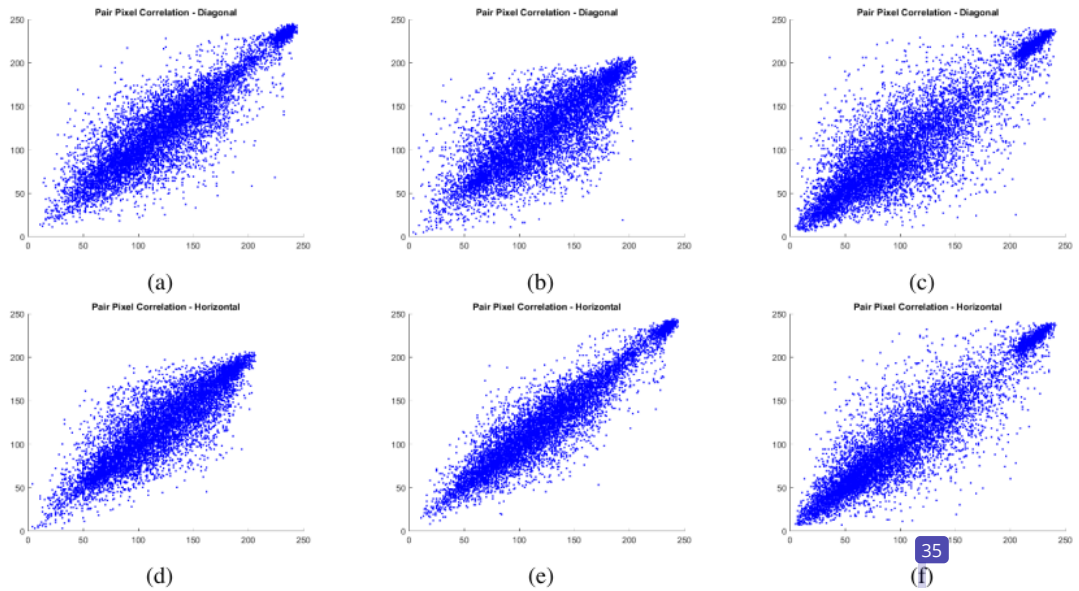
Image	Method	Red	Green	Blue	Average RGB
Lena	[11]	7.9974	7.9977	7.9970	7.9974
	[8]	7.9970	7.9970	7.9976	7.9972
	[18]	7.9951	7.9965	7.9829	7.9915
	[53]	7.9974	7.9975	7.9973	7.9974
	Ours	7.9976	7.9978	7.9976	7.9977
Baboon	[8]	7.9974	7.9968	7.9970	7.9971
	[18]	7.9973	7.9974	7.9975	7.9974
	Ours	7.9977	7.9976	7.9978	7.9977
Peppers	[8]	7.9970	7.9974	7.9973	7.9972
	[18]	7.9972	7.9969	7.9973	7.9971
	[53]	7.9974	7.9974	7.9975	7.9974
	Ours	7.9977	7.9975	7.9977	7.9976
House	[11]	7.9970	7.9974	7.9972	7.9972
	Ours	7.9976	7.9977	7.9978	7.9977
Jelly Beans	[11]	7.9972	7.9972	7.9977	7.9974
	Ours	7.9975	7.9977	7.9978	7.9977
Tree	[11]	7.9976	7.9971	7.9971	7.9973
	Ours	7.9977	7.9978	7.9975	7.9977

C. CORRELATION COEFFICIENT OF ADJACENT PIXEL ANALYSIS

The correlation coefficient of adjacent pixels (r) in image encryption is a method used to measure the level of dependence between adjacent pixels in an image. This is important in image encryption because if there is a high dependence between pixels, the image can be easily predicted and vulnerable to attacks, especially statistical attacks[56]. The range of the r value is from minus one to one. A value of -1 indicates a perfect negative correlation between two pixels, a value of zero indicates no correlation between two pixels, and a value of one indicates a perfect positive correlation between two pixels. The r value in plain images generally deviates from zero, while it should close to zero after encryption. Eq. (9) is used to assess the r value.

$$r_{x,y} = \frac{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]}{\sqrt{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2}\sqrt{\frac{1}{N}\sum_{i=1}^{N}[y_i - E(y)]^2}} \quad (9)$$

The symbol N in Eq. (9) represents the total number of pixels in an image, whereas x and y denote two adjacent pixels in the diagonal, horizontal, or vertical direction. The expectations of x and y are represented by $E(x)$ and $E(y)$, respectively, and the correlation coefficient of adjacent pixels is denoted by r. Fig. 7 illustrates the correlation coefficient plot of 10,000 pairs of pixels for each direction (horizontal, vertical, and diagonal) and each channel of both plain and encrypted images. Table 6 shows the results of measuring r in each horizontal, vertical, and diagonal. These results validate that the proposed method has successfully reduced the value of r to nearly zero, which is even superior to the previous method (refer to Table 7).



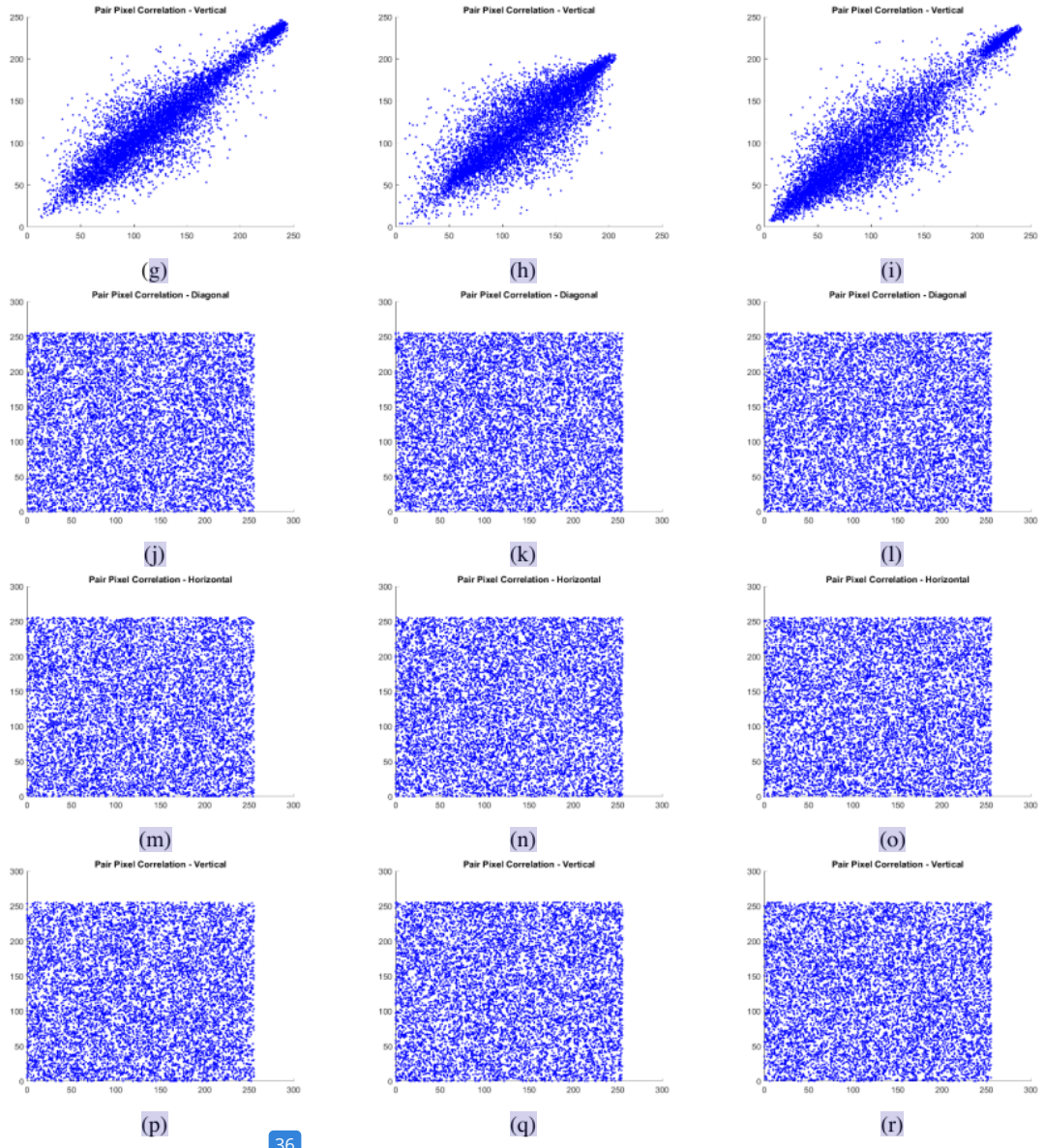


FIGURE 7. Sample Plot of Pixel Pair Correlation of Baboon image {(a, b, c) Red, Green, Blue Plain Diagonal Correlation, respectively; (d, e, f) Red, Green, Blue Plain Horizontal Correlation, respectively; (g, h, i) Red, Green, Blue Plain Vertical Correlation, respectively; (j, k, l) Red, Green, Blue Cipher Diagonal Correlation, respectively; (e) Red, Green, Blue Cipher Horizontal Correlation, respectively; (f) Red, Green, Blue Cipher Vertical Correlation, respectively}

TABLE VI
CORRELATION COEFFICIENT RESULTS

Image	Direction	Color Chanel		
		Red	Green	Blue
Lena	D	-0.0015	0.0013	-0.0017
	H	0.0002	-0.0010	-0.0018
	V	0.0018	0.0017	0.0001
Baboon	D	-0.0006	-0.0006	0.0011
	H	0.0003	-0.0012	0.0017
	V	-0.0011	-0.0010	-0.0015
Peppers	D	0.0010	0.0005	0.0003
	H	-0.0010	-0.0001	-0.0001
	V	0.0001	-0.0006	-0.0020
Jelly Beans	D	0.0008	0.0013	-0.0007
	H	0.0016	0.0003	-0.0014
	V	0.0018	0.0002	0.0012
House	D	0.0002	0.0017	-0.0008
	H	-0.0014	-0.0009	0.0001
	V	-0.0014	0.0010	-0.0013
Tree	D	-0.0010	0.0010	0.0004
	H	0.0014	-0.0005	-0.0009
	V	-0.0010	0.0003	0.0006

TABLE VII
CORRELATION COEFFICIENT COMPARISON WITH THE PREVIOUS METHOD

Image	Method	Direction	Red	Green	Blue
Lena	[11]	D	0.0011	0.0014	0.0018
		H	0.0032	-0.0032	−0.0019
		V	−0.0012	−0.0039	0.0013
	[8]	D	-0.0043	0.0026	0.0008
		H	0.0071	-0.0005	-0.0029
		V	0.0009	-0.0034	0.0045
	Ours	D	-0.0015	0.0013	-0.0017
		H	0.0002	-0.0010	-0.0018
		V	0.0018	0.0017	0.0001
Peppers	[54]	D	−0.0013	0.0010	−0.0007
		H	0.0010	0.0030	0.0033
		V	0.0026	0.0003	−0.0010
	Ours	D	0.0010	0.0005	0.0003
		H	-0.0010	-0.0001	-0.0001
		V	0.0001	-0.0006	-0.0020

D. DIFFERENTIAL ANALYSIS

The commonly used statistical measurement tool for determining the resistance of image encryption against differential attacks is Normalized Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)[37]. Its function measures the difference between two encrypted images, where the first image is the default encrypted image and the second is a 1-bit modified image of the plaintext before encryption[57]. NPCR calculates the percentage of pixel changes between the two encrypted images, with an ideal value of ≈ 99.6094%. The ideal NPCR value is calculated from the 1-bit difference for every 256 pixels in the encrypted image. Meanwhile, UACI measures the average intensity of changes between two encrypted images, with an ideal value of ≈ 33.4635%. The ideal UACI value is calculated from the 1-bit difference for every 3 pixels in the encrypted image[58]. Eq. (10) and (11) are used to evaluate UACI and NPCR.

TABLE VIII
NPCR AND NPCR RESULTS

Image	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lena	99.6066	99.6040	99.6046	33.4887	33.4987	33.4907
Baboon	99.6105	99.6058	99.5887	33.4350	33.5029	33.4972
Peppers	99.6034	99.6055	99.5945	33.5249	33.4165	33.4292
Jelly Beans	99.5888	99.5972	99.5891	33.3949	33.4595	33.4865
House	99.6080	99.6034	99.5903	33.4523	33.4533	33.4830
Tree	99.6099	99.5920	99.6074	33.4442	33.4818	33.4131
Average	99.6046	99.6013	99.5958	33.4567	33.4688	33.4666

TABLE IX
NPCR AND UACI COMPARISON WITH PREVIOUS METHOD

Image	Method	NPCR			UACI		
		Red	Green	Blue	Red	Green	Blue
Lena	[11]	99.6048	99.6216	99.6414	33.5047	33.3756	33.5031
	[8]	99.6216	99.6277	99.6189	33.4032	33.5997	33.4912
	[18]	99.6100	99.5800	99.6200	33.3600	33.4900	33.5000
	[53]	99.6155	99.6017	99.6048	33.5200	33.4688	33.4671
	Ours	99.6066	99.6040	99.6046	33.4887	33.4987	33.4907
Baboon	[8]	99.6470	99.6372	99.6109	33.6047	33.4579	33.4247
	[18]	99.5900	99.5800	99.5700	33.3700	33.3900	33.5600
	Ours	99.6105	99.6058	99.5887	33.4350	33.5029	33.4972
Peppers	[8]	99.6872	99.6489	99.6117	33.4029	33.4851	33.5216
	[18]	99.6000	99.5700	99.5600	33.5200	33.5700	33.6300
	Ours	99.6034	99.6055	99.5945	33.5249	33.4165	33.4292
House	[8]	99.6155	99.6297	99.6267	33.4144	33.6090	33.4248
	[11]	99.6048	99.6216	99.6414	33.5047	33.3756	33.5031
	Ours	99.6080	99.6034	99.5903	33.4523	33.4533	33.4830
Jelly beans	[8]	99.6143	99.6302	99.6140	33.4069	33.6900	33.4726
	[11]	99.6567	99.5865	99.6292	33.4501	33.4492	33.5508
	Ours	99.5888	99.5972	99.5891	33.3949	33.4595	33.4865
Tree	[8]	99.6185	99.6238	99.6395	33.68.58	33.6383	33.5260
	[11]	99.6292	99.6033	99.6292	33.4070	33.4116	44.4639
	Ours	99.6099	99.5920	99.6074	33.4442	33.4818	33.4131

$$NPCR = \left[\frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H} Diff(i,j)\right], \quad (10)$$

$$Diff(i,j)\begin{cases}0 \text{ if } C1(i,j) = C2(i,j)\\ 1 \text{ if } C1(i,j) \neq C2(i,j)\end{cases}$$

$$UACI = \left[\frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \quad (11)$$

Where $C1$ and $C2$ represent default cipher and modified cipher, respectively, W and H represent the width and the height dimension respectively, i and j both are pixel coordinates. The NPCR and UACI results are shown in Table 8, while Table 9 compares with previous research. Based on the results in these tables, most NPCR and UACI values seem closer to the ideal value than the previous work. This indicates that the proposed method has better encryption performance, particularly in preventing differential attacks.

E. PEAK SIGNAL-TO-NOISE RATIO (PSNR) AND BIT ERROR RATIO (BER) ANALYSIS

Another common measure used in image encryption is PSNR and BER. PSNR statistically assesses the level of noise that distorts the encrypted image, where if the level of distortion is high, it indicates that the encryption works well[8], [54]. Similarly, the BER evaluation can determine how large the bit error rate is in the encrypted image. Both evaluations compare the plain image and the encrypted image to calculate it, where the closer it is to zero, the better the PSNR. Conversely, the BER value must be larger to provide the same indication. PSNR and BER can each be evaluated with Eq. (12) and (13), respectively.

$$PSNR_{OC} = 10\log 10\left(\frac{max^2}{\frac{1}{WHS}\sum_{i=1}^{W}\sum_{j=1}^{H}\sum_{s=1}^{S}(O_{ijs} - C_{ijs})^2}\right) \quad (12)$$

$$BER_{OC} = \frac{\sum_{i=1}^{L} O_i \veebar C_i}{L_O} \times 100\% \quad (13)$$

Where O and C are original and ciphered images, respectively, W,H, and S are their respective width, height, and layer or color space dimensions, i, j, and s represent the corresponding pixel coordinates. At the same time, max is the maximum pixel value of O and C. The formula for BER

uses i as an index because the image is first transformed to a binary form and then reshaped into a one-dimensional array, L is bit length, where e both must be the same.

In this section, measurement is also conducted on the decryption process. The decryption process is performed by reversing the encryption steps. The output of this process is the decrypted image, which should be identical to the original image to prove that the decryption process works perfectly. The decryption process with errors can cause noise in the image. To assess it, the measurement tools such as PSNR and BER can also be used in this stage. The process is the same as the encryption process, but the original image and the decrypted image are compared, and the PSNR measurement result should be ∞, while the BER should be 0 to validate the perfect decryption result. Table 10 displays the results of PSNR and BER evaluations in both the encryption and decryption stages. Meanwhile, Table 11 compares the PSNR values with the previous method. The presented results show that most of the PSNR values generated are better because they are smaller, indicating greater distortion on the encrypted image. While the PSNR and BER values in the decryption process show that the decryption process can work perfectly

TABLE X
PSNR AND BER RESULTS IN ENCRYPTION AND DECRYPTION

Image	Encryption		Decryption	
	PSNR	BER (%)	PSNR	BER (%)
Lena	7.0257	50.5036	∞	0
Baboon	7.1515	51.8955	∞	0
Peppers	6.5166	51.3013	∞	0
Jelly Beans	5.7343	52.2475	∞	0
House	6.0440	50.3503	∞	0
Tree	7.5038	51.1036	∞	0
Average	6.6626	51.2336	∞	0

TABLE XI
PSNR OF ENCRYPTION COMPARISON

Image	Method [32]	Method [8]	Method [54]	Ours
Lena	8.5786	7.8694	-	7.0257
Baboon	8.8048	8.7855	-	7.1515
Peppers	-	9.0991	8.1257	6.5166
Jelly Beans	-	8.4897	-	5.7343
House	-	9.8163	-	6.0440
Tree	-	8.6982	-	7.5038

F. KEYSPACE AND KEY SENSITIVITY ANALYSIS

Keyspace refers to the range of all possible encryption keys used in a particular encryption system. In image encryption analysis, key space is crucial because the larger the keyspace, the more difficult it is to guess the correct encryption key. In a good encryption system, the keyspace should be large enough to make brute-force attacks impractical. In the [59], [60] studies, it was stated that at least 2^{100} is required to make brute-force attacks impractical. The proposed method uses several initial value parameters that can be dynamically set and hash functions to increase the keyspace. A detailed calculation of the keyspace is presented in Table 12.

TABLE XII
KEYSPACE APPROXIMATION FOR ALL PHASE

Method	Keyspace
SHA-512	2^{512}
Improve Logistic Map	$\approx 0.9999999998 \times 10^{15} \approx 10^{16}$
6D Hyperchaotic System	$\approx 6 \times 10^{16}$
Total	$\approx 2^{512} + 7 \times 10^{16}$

The data presented in Table 12 shows that the possible key space in this method is approximately $\approx 2^{512} + 7 \times 10^{16}$, this should confirm that the proposed method resists brute-force attacks. The sensitivity key on image encryption is a test to examine how sensitive the image encryption is changes in the encryption key. In image encryption, the original image is transformed into an encrypted image using an encryption key. In the key sensitivity test, variations are made to the encryption key to observe its influence on the resulting encrypted image. The key sensitivity test is important to maintain the security of the encrypted image from attacks if the encryption key is leaked or accessed by unauthorized parties. The difference between the encrypted image with the original key and the modified key is used to determine the sensitivity of the key in image encryption. The sensitivity test in this research was conducted by modifying a 1-bit key in the decryption process. In Fig. 8, it is visually clear that the encrypted result is significantly different. This is due to the dynamic key parameters and chaotic sequence being highly sensitive to changes, combined with the SHA-512 function, resulting in a compounded effect on key sensitivity.

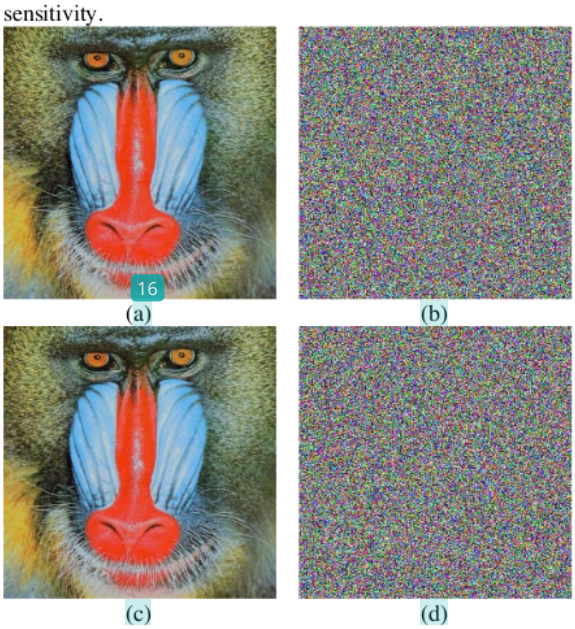


FIGURE 8. Sample of Key Sensitivity Decryption Results{(a) Original Baboon Image; (b) Encrypted Baboon Image; (c) Decrypted Baboon Image with correct key;(d) Decrypted Baboon Image with slight key modification}

G. NIST RANDOMNESS TEST

The NIST randomness test checks whether a sequence of random numbers meets the randomness standards set by the National Institute of Standards and Technology (NIST). This function is often used to test the keys' randomness in cryptographic algorithms. In image encryption, the NIST randomness test function ensures that the keys used in the image encryption process are random and unpredictable[61]. The suite of tests (SP 800-22) is available for download at https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. It comprises 15 tests designed to analyze random bit sequences' behavior. A p-value in the range of [0...1] is generated for each test. To validate the encryption and pass the test, each test requires a minimum of 106-bit sequences that produce a p-value greater than 0.01[56]. The image is first converted into a binary file to conduct the test and saved with a .dat extension. Table 13 displays the test results, including the average p-value of all encrypted images. The NIST statistical test results demonstrate that the proposed method successfully passes all tests and is resilient to various types of attacks.

TABLE XIII
NIST STATISTICAL TEST SUITE RESULTS

No	Test Name	p-Value	Note
1	Frequency	0.753319	Passed
2	Block Frequency	0.612014	Passed
3 a	Cumulative Sums (Forward)	0.544545	Passed
3 b	Cumulative Sums (Reverse)	0.772219	Passed
4	Runs	0.890363	Passed
5	Longest Run of Ones	0.779176	Passed
6	Rank	0.690237	Passed
7	Discrete Fourier Transform	0.721648	Passed
8	Nonperiodic Template Matchings	0.791120	Passed
9	Overlapping Template Matchings	0.861762	Passed
38	Universal Statistical	0.432321	Passed
11	Approximate Entropy	0.360523	Passed
12	Random Excursions	0.869847	Passed
13	Random Excursions Variant	0.646304	Passed
14	Serial	0.559851	Passed
15	Linear Complexity	0.873263	Passed
	Average	0.697407	Passed

H. DATA LOSS AND NOISE ATTACK

Image encryption is the process of converting the original image into an encrypted image that cannot be read by people who do not have the encryption key. However, when encrypted images are transmitted, they can be vulnerable to data loss and noise attacks. Data loss attacks occur when some of the data in encrypted images is lost due to transmission or storage errors. This can cause the encrypted image to become unreadable or even corrupt. Meanwhile, noise attacks occur when data in encrypted images are corrupted with additional unwanted data, such as noise or wrong signals. This can cause encrypted images to become unreadable or difficult to read.

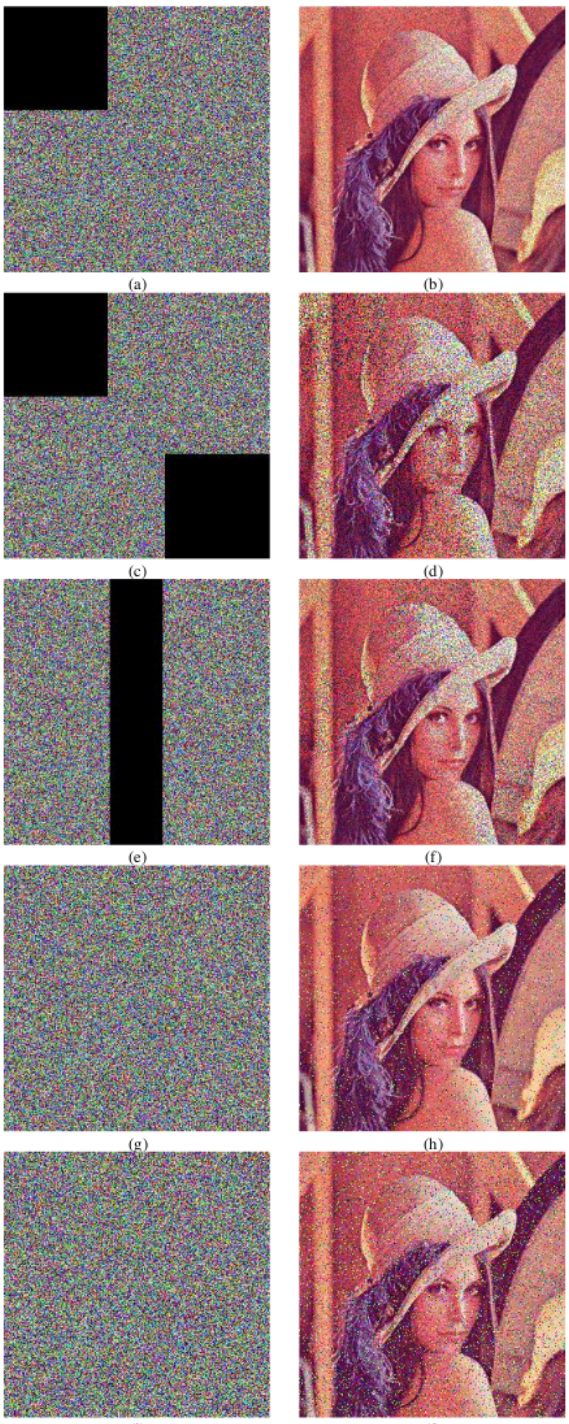


FIGURE 9. Sample of Encrypted and Decrypted Image after Attack {(a, c) Encrypted Lena Image after Data Loss Attack; (b, d, f) Decrypted Lena Image after Data Loss Attack; (g, i) Encrypted Lena Image after Noise Attack; (h, j) Decrypted Lena Image after Noise Attack; }

Data loss and noise attack tests are significant in image encryption methods because they help identify the resistance level of encrypted images against these attacks. Suppose the encrypted image can withstand the attack. In that case, it means that the encrypted image has a better level of security and can be considered for use in more sensitive security applications. In this section, a sample of the results of a data loss attack is presented with a loss of 100 × 100, 2 × 100 × 100, and 50 × 256 pixels. This is equivalent to data loss of ≈ 15.26%, ≈ 30.52%, and ≈ 19.53%, respectively. At the same time, the noise test is tested using a salt and pepper attack with a density of 0.05 and 0.1, respectively, which are presented in Fig. 9. If measured by PSNR, the decrypted image is no more than 20dB, but visually, it appears that the image decryption results can still be recognized as the original image even though there is noise. In addition, even though in the data loss test, the loss is concentrated in certain parts of the data, the results of the decryption data loss spread evenly throughout the image. This makes the proposed encryption method resistant to data loss and noise attacks.

I. ENERGY, CONTRAST, AND HOMOGENEITY ANALYSIS

In some image encryption research[20], [62], several image features such as energy, homogeneity, and contrast can indicate encryption quality. A lower energy value in the cipher indicates higher interference from the cipher image. In other words, it can mean better encryption quality. Contrast analysis can be used to evaluate the difference in intensity between pixels and their neighbors in the whole image. A higher contrast value indicates a more uneven texture, so it can be interpreted that the quality of the image encryption is better in this case. Meanwhile, homogeneity analysis is used to measure the closeness of the distribution on the gray-level co-occurrence matrices (GLCM). Thus the cipher image that has a lower homogeneity value generally has higher security. Energy, contrast, and homogeneity can each be calculated by Eq. (14), (15), and (16).

$$Energy = \sum_{i,j} p(i,j)^2 \tag{14}$$

$$Contrast = \sum_{i,j} |i-j|^2 \times p(i,j) \tag{15}$$

$$Homogeneity = \sum_{i,j} \frac{p(i,j)}{1+|i-j|} \tag{16}$$

Where $p(i,j)$ represents the number of GLCM, in this study, the three features are measured at each layer (red, green, and blue), because GLCM is generally calculated on grayscale images or 8 bits images. The measurement results for these three features are presented in Table 14.

TABLE XIV
AVERAGE ENERGY, CONTRAST, AND HOMOGENEITY ANALYSIS RESULTS OF ENCRYPTED IMAGE

Feature	Red	Green	Blue	Average
Contrast	10.6584	10.7028	10.6437	10.6683
Energy	0.0192	0.0202	0.0171	0.0188
Homogeneity	0.3913	0.3789	0.4011	0.3904

Based on the energy, contrast, and homogeneity analysis results, the results are relatively commensurate with research [20], where the sample pepper color image yielded homogeneity = 0.3906, contrast = 10.4840, and energy = 0.016. But these results are clearly superior to research [62], where the homogeneity value = 0.4110, contrast = 10.1098, and energy = 0.165. This proves that the proposed method has relatively good quality based on these three features.

V. CONCLUSION

This study succeeded in designing an encryption algorithm that combines several diffusion patterns and interleaved confusion based on a combination of chaotic maps, namely 6D hyperchaotic and 1D chaotic systems. The goal is to increase security by spreading encryption evenly throughout the image and providing high encryption complexity so it is not easy to decrypt. The 1D Chaotic map has a positive LE value which is intended to provide unstable dynamics, making it more sensitive to initial conditions. In the first stage, the encryption algorithm provides a uniform encryption effect, as evidenced by an identical histogram for each channel but different from the original. The second, third, and fourth stages use the 6D hyperchaotic system. This hyperchaotic has four positive LE values, one zero LE, and one negative LE, resulting in a very dynamic, robust, and unpredictable chaotic sequence. Six chaotic sequences were used for the three stages of encryption with alternating diffusion and obfuscation patterns with different interleaved techniques and scan patterns. The SHA-512 algorithm is also implemented to improve keyspace quality and key sensitivity. Based on the hypothesis, this approach succeeded in designing an encryption algorithm resistant to various attack tests such as statistical, differential, brute force, NIST randomness, data loss, and noise attacks. Moreover, the proposed method yields superior results over the previous method.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] J. S. Khan, J. Ahmad, S. F. Abbasi, Arshad, and S. K. Kayhan, "DNA Sequence Based Medical Image Encryption Scheme," *2018 10th Comput. Sci. Electron. Eng. Conf. CEEC 2018 - Proc.*, pp. 24–29, 2019, doi: 10.1109/CEEC.2018.8674221.

[2] J. S. Khan, J. Ahmad, S. S. Ahmed, H. A. Siddiqa, S. F. Abbasi, and S. K. Kayhan, "DNA key based visual chaotic image encryption," *J. Intell. Fuzzy Syst.*, vol. 37, no. 2, pp. 2549–2561, Sep. 2019, doi: 10.3233/JIFS-182778.

[3] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital Image Steganography Survey and Investigation (Goal, Assessment, Method, Development, and Dataset)," *Signal*

Processing, vol. 206, p. 108908, May 2023, doi: 10.1016/j.sigpro.2022.108908.

[4] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, no. September 2018, pp. 163–185, Nov. 2019, doi: 10.1016/j.sigpro.2019.06.010.

[5] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion Based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. November, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[6] Q. Qin, Z. Liang, S. Liu, X. Wang, and C. Zhou, "A Dual-domain Image Encryption Algorithm Based on Hyperchaos and Dynamic Wavelet Decomposition," *IEEE Access*, vol. 10, no. October, pp. 122726–122744, 2022, doi: 10.1109/ACCESS.2022.3212145.

[7] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing," *IEEE Access*, vol. 8, pp. 210382–210399, 2020, doi: 10.1109/ACCESS.2020.3039891.

[8] M. G. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020, doi: 10.1109/ACCESS.2020.2990170.

[9] M. Hanif *et al.*, "A Novel and Efficient Multiple RGB Images Cipher Based on Chaotic System and Circular Shift Operations," *IEEE Access*, vol. 8, pp. 146408–146427, 2020, doi: 10.1109/ACCESS.2020.3015085.

[10] D. R. I. M. Setiadi, E. H. Rachmawanto, and R. Zulfiningrum, "Medical Image Cryptosystem using Dynamic Josephus Sequence and Chaotic-hash Scrambling," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6818–6828, Oct. 2022, doi: 10.1016/j.jksuci.2022.04.002.

[11] M. Wang, X. Wang, C. Wang, S. Zhou, Z. Xia, and Q. Li, "Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing," *Digit. Signal Process.*, vol. 132, p. 103818, 2022, doi: 10.1016/j.dsp.2022.103818.

[12] A. K. Shibeeb, M. H. Ahmed, and A. H. Mohammed, "A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation," *Karbala Int. J. Mod. Sci.*, vol. 7, no. 3, pp. 176–188, 2021, doi: 10.33640/2405-609X.3117.

[13] A. Kadhim and R. S. Ali, "Enhancement AES based on 3D Chaos Theory and DNA Operations Addition," *Karbala Int. J. Mod. Sci.*, vol. 5, no. 2, pp. 112–118, Jul. 2019, doi: 10.33640/2405-609X.1137.

[14] S. Mansoor and S. A. Parah, "HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing," *Multimed. Tools Appl.*, Feb. 2023, doi: 10.1007/s11042-023-14542-7.

[15] W. Feng and J. Zhang, "Cryptanalzing a Novel Hyper-Chaotic Image Encryption Scheme Based on Pixel-Level Filtering and DNA-Level Diffusion," *IEEE Access*, vol. 8, pp. 209471–209482, 2020, doi: 10.1109/ACCESS.2020.3038006.

[16] W. Feng, Z. Qin, J. Zhang, and M. Ahmad, "Cryptanalysis and Improvement of the Image Encryption Scheme Based on Feistel Network and Dynamic DNA Encoding," *IEEE Access*, vol. 9, pp. 145459–145470, 2021, doi: 10.1109/ACCESS.2021.3123571.

[17] W. Feng, Y. G. He, H. M. Li, and C. L. Li, "Cryptanalysis of the integrated chaotic systems based image encryption algorithm," *Optik (Stuttg).*, vol. 186, no. November 2018, pp. 449–457, 2019, doi: 10.1016/j.ijleo.2018.12.103.

[18] S. M. Basha, P. Mathivanan, and A. B. Ganesh, "Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map," *Optik (Stuttg).*, vol. 259, no. November 2021, 2022, doi: 10.1016/j.ijleo.2022.168956.

[19] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual Meaningful Encryption Scheme Using Intertwinning Logistic Map," in *Intelligent Computing*, 2019, pp. 764–773.

[20] H. Li *et al.*, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion," *J. Inf. Secur. Appl.*, vol. 61, no. June, p. 102844, Sep. 2021, doi: 10.1016/j.jisa.2021.102844.

[21] W. Feng, Y. He, H. Li, and C. Li, "A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm," *IEEE Access*, vol. 7, pp. 181589–181609, 2019, doi: 10.1109/ACCESS.2019.2959137.

[22] D. R. I. M. Setiadi, R. Zulfiningrum, E. H. Rachmawanto, and P. N. Andono, "Medical Image Encryption Using Bit Plane Slicing , Dynamic Chaos , and Hash Function," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 6, pp. 293–302, 2022, doi: 10.22266/ijies2022.1231.28.

[23] L. Kocarev and S. Lian, *Chaos-Based Cryptography*, vol. 354. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. doi: 10.1007/978-3-642-20542-2.

[24] J. Katz and Y. Lindell, "Introduction to modern cryptography," *Introd. to Mod. Cryptogr.*, pp. 1–527, 2007, doi: 10.1201/b17668.

[25] M. W. Hirsch, S. Smale, and R. L. Devaney, *Differential Equations, Dynamical Systems, and an Introduction to Chaos*. Elsevier, 2013. doi: 10.1016/C2009-0-61160-0.

[26] M. Ahmad *et al.*, "An image encryption algorithm based on new generalized fusion fractal structure," *Inf. Sci. (Ny).*, vol. 592, pp. 1–20, 2022, doi: 10.1016/j.ins.2022.01.042.

[27] U. Erkan, A. Toktas, and Q. Lai, "2D hyperchaotic system based on Schaffer function for image encryption," *Expert Syst. Appl.*, vol. 213, no. October 2022, 2023, doi: 10.1016/j.eswa.2022.119076.

[28] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," *J. Adv. Res.*, vol. 10, pp. 85–98, Mar. 2018, doi: 10.1016/j.jare.2018.01.009.

[29] M. García-Martínez, L. J. Ontañón-García, E. Campos-Cantón, and S. Čelikovský, "Hyperchaotic encryption based on multi-scroll piecewise linear systems," *Appl. Math. Comput.*, vol. 270, pp. 413–424, 2015, doi: 10.1016/j.amc.2015.08.037.

[30] L. Yang, Q. Yang, and G. Chen, "Hidden attractors, singularly degenerate heteroclinic orbits, multistability and physical realization of a new 6D hyperchaotic system," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 90, 2020, doi: 10.1016/j.cnsns.2020.105362.

[31] R. R. Suman, B. Mondal, and T. Mandal, "A secure encryption scheme using a Composite Logistic Sine Map (CLSM) and SHA-256," *Multimed. Tools Appl.*, pp. 27089–27110, 2022, doi: 10.1007/s11042-021-11460-4.

[32] T. ul Haq and T. Shah, "4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion," *J. Inf. Secur. Appl.*, vol. 61, no. July, p. 102931, 2021, doi: 10.1016/j.jisa.2021.102931.

[33] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal, "A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations," *IEEE Access*, vol. 8, pp. 123536–123555, 2020, doi: 10.1109/ACCESS.2020.3004536.

[34] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017, doi: 10.1016/j.optlaseng.2016.10.020.

[35] S. K.U. and A. Mohamed, "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion," *Signal Process. Image Commun.*, vol. 99, no. May, p. 116495, 2021, doi: 10.1016/j.image.2021.116495.

[36] K. Qian, W. Feng, Z. Qin, J. Zhang, X. Luo, and Z. Zhu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Front. Phys.*, vol. 10, no. August, pp. 1–19, 2022, doi: 10.3389/fphy.2022.963795.

[37] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Expert Syst. Appl.*, vol. 213, no. PB, p. 119074, 2023, doi: 10.1016/j.eswa.2022.119074.

[38] K. U. Shahna and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Appl. Soft Comput. J.*, vol. 90, p. 106162, May 2020, doi: 10.1016/j.asoc.2020.106162.

[39] A. Belazi *et al.*, "Improved Sine-Tangent chaotic map with application in medical images encryption," *J. Inf. Secur. Appl.*, vol. 66, no. March, p. 103131, 2022, doi: 10.1016/j.jisa.2022.103131.

[40] M. Hussain, N. Iqbal, and Z. Bashir, "A chaotic image encryption scheme based on multi-directional confusion and diffusion operations," *J. Inf. Secur. Appl.*, vol. 70, no. October, p. 103347, 2022, doi: 10.1016/j.jisa.2022.103347.

[41] X. Wang and M. Zhang, "An image encryption algorithm based on new chaos and diffusion values of a truth table," *Inf. Sci. (Ny).*, vol. 579, pp. 128–149, 2021, doi: 10.1016/j.ins.2021.07.096.

[42] W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, and Y. He, "Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform," *Mathematics*, vol. 10, no. 15, pp. 1–24, 2022, doi: 10.3390/math10152751.

[43] Z. hua Gan, X. li Chai, D. jun Han, and Y. ran Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, 2019, doi: 10.1007/s00521-018-3541-y.

[44] J. Yu, W. Xie, Z. Zhong, and H. Wang, "Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation," *Chaos, Solitons and Fractals*, vol. 162, no. February, p. 112456, 2022, doi: 10.1016/j.chaos.2022.112456.

[45] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci. (Ny).*, vol. 349–350, pp. 137–153, 2016, doi: 10.1016/j.ins.2016.02.041.

[46] G. Grassi, F. L. Severance, and D. A. Miller, "Multi-wing hyperchaotic attractors from coupled Lorenz systems," *Chaos, Solitons and Fractals*, vol. 41, no. 1, pp. 284–291, 2009, doi: 10.1016/j.chaos.2007.12.003.

[47] S. Strogatz, *Nonlinear dynamics and chaos : with applications to physics, biology, chemistry, and engineering*. Second edition. Boulder, CO : Westview Press, a member of the Perseus Books Group, [2015]. [Online]. Available: https://search.library.wisc.edu/catalog/9910223127702121

[48] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik (Stuttg).*, vol. 181, no. December 2018, pp. 779–785, 2019, doi: 10.1016/j.ijleo.2018.12.178.

[49] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Lasers Eng.*, vol. 107, pp. 370–379, Aug. 2018, doi: 10.1016/J.OPTLASENG.2017.06.015.

[50] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Inf. Sci. (Ny).*, vol. 593, pp. 121–154, 2022, doi: 10.1016/j.ins.2022.01.031.

[51] U. Erkan, A. Toktas, F. Toktas, and F. Alenezi, "2D eπ-map for image encryption," *Inf. Sci. (Ny).*, vol. 589, pp. 770–789, 2022, doi: 10.1016/j.ins.2021.12.126.

[52] National Institute of Standards and Technology, "Secure Hash Standard," Gaithersburg, MD, Jul. 2015. doi: 10.6028/NIST.FIPS.180-4.

[53] S. Wang, Q. Peng, and B. Du, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Opt. Laser Technol.*, vol. 148, no. November 2021, p. 107753, 2022, doi: 10.1016/j.optlastec.2021.107753.

[54] D. Li, J. Li, and X. Di, "A novel exponential one-dimensional chaotic map enhancer and its application in an image encryption scheme using modified ZigZag transform," *J. Inf. Secur. Appl.*, vol. 69, no. August, p. 103304, 2022, doi: 10.1016/j.jisa.2022.103304.

[55] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 333–350, 2020, doi: 10.1016/j.future.2020.02.029.

[56] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, no. November 2022, p. 170316, 2023, doi: 10.1016/j.ijleo.2022.170316.

[57] W. Feng, Y. G. He, H. M. Li, and C. L. Li, "Image encryption algorithm based on discrete logarithm and memristive chaotic system," *Eur. Phys. J. Spec. Top.*, vol. 228, no. 10, pp. 1951–1967, 2019, doi: 10.1140/epjst/e2019-800209-3.

[58] Y. Zhang, "Statistical test criteria for sensitivity indexes of image cryptosystems," *Inf. Sci. (Ny).*, vol. 550, pp. 313–328, 2021, doi: 10.1016/j.ins.2020.10.026.

[59] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017, doi: 10.1016/j.sigpro.2017.04.006.

[60] Y. Liu and J. Zhang, "A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding," *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21579–21601, 2020, doi: 10.1007/s11042-020-08880-z.

[61] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Fort Belvoir, 2001. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA393366

[62] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Jan. 2017, doi: 10.3233/JIFS-17656.

EDY WINARNO received a Doctoral degree in Computer Science from the Department of Computer Science Gadjah Mada University in 2016. He is currently an Associate Professor at the Faculty of Information Technology and Industry at Stikubank University. His research interests include computer vision, image processing and security, and artificial intelligence. He can be contacted at email: edywin@edu.unisbank.ac.id..

KRISTIAWAN NUGROHO is a lecturer and researcher at the Faculty of Information Technology and Industry, Stikubank University. He obtained a bachelor's degree in 2001 in the information systems department, Faculty of Computer Science, Dian Nuswantoro University. In 2007, he obtained a Master's degree in Informatics Engineering from Dian Nuswantoro University. He also obtained a Doctoral degree in Computer Science with a concentration in Machine Learning and Artificial Intelligence in 2022 at Dian Nuswantoro University Semarang. He has researched machine learning, image recognition, speech recognition, and sentiment analysis. He can be contacted via email at kristiawan@edu.unisbank.ac.id

PRAJANTO WAHYU ADI received the Bachelor in computer science from Universitas Stikubank, Indonesia in 2011. He finished his master's degree through a dual degree program in information technology at Universitas Dian Nuswantoro, Indonesia and in the field of computer science at the Universiti Teknikal Malaysia Melaka, Malaysia, in 2014. He served as a lecturer at the Department of Information Technology, Faculty of Computer Science, Universitas Dian Nuswantoro and currently works as a lecturer at the Department of Informatics, Faculty of Science and Mathematics, Universitas Diponegoro. His areas of expertise are cryptography, digital image classification, steganography, and watermarking. He can be contacted at email: prajanto@live.undip.ac.id

DE ROSAL IGNATIUS MOSES SETIADI received a Bachelor's degree from the Department of Informatics Engineering Soegijapranata Catholic University, Semarang Indonesia, in 2010 and a Master's degree in the Department of Informatics Engineering Dian Nuswantoro University, Semarang, Indonesia, in 2012. He is a lecturer and researcher at the Faculty of Computer Science, Dian Nuswantoro University, Semarang, Indonesia. He has authored or co-authored more than 139 refereed journal and conference papers indexed by Scopus. He is one of the academic editors in the Security and Communication Journal and Journal of Computer Networks and Communications Hindawi and one of the editorial board in the TEM (Technology, Education, Management, Informatics) Journal. He is also a reviewer of more than 50 Scopus-indexed journals. His research interests include image encryption, cryptography, steganography, watermarking, and image recognition. He can be contacted at email: moses@dsn.dinus.ac.id.

Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption based on Hyperchaotic System

ORIGINALITY REPORT

21%	16%	17%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	1%
2	Submitted to University of Macau Student Paper	1%
3	www.hindawi.com Internet Source	1%
4	www.mdpi.com Internet Source	1%
5	Mingxu Wang, Xingyuan Wang, Chunpeng Wang, Shuang Zhou, Zhiqiu Xia, Qi Li. "Color image encryption based on 2D enhanced hyperchaotic logistic-sine map and two-way Josephus traversing", Digital Signal Processing, 2022 Publication	1%
6	www.researchgate.net Internet Source	1%
7	Haidar Raad Shakir. "A Color-Image Encryption Scheme Using a 2D Chaotic	1%

System and DNA Coding", Advances in Multimedia, 2019
Publication

8	Congxu Zhu, Kehui Sun. "Cryptanalyzing and Improving a Novel Color Image Encryption Algorithm Using RT-Enhanced Chaotic Tent Maps", IEEE Access, 2018 Publication	1 %
9	Submitted to Indian Institute of Technology Student Paper	1 %
10	Submitted to Suleyman Demirel University, Kazakhstan Student Paper	1 %
11	mdpi-res.com Internet Source	1 %
12	univ-usto.dz Internet Source	1 %
13	Submitted to Universiti Kebangsaan Malaysia Student Paper	<1 %
14	Yucheng Chen, Chunming Tang, Ruisong Ye. "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Processing, 2020 Publication	<1 %

15	Xingyuan Wang, Wenhua Xue, Jubai An. "Image encryption algorithm based on Tent-Dynamics coupled map lattices and diffusion of Household", Chaos, Solitons & Fractals, 2020 Publication	<1 %
16	ijece.iaescore.com Internet Source	<1 %
17	Pulung Nurtantio Andono, De Rosal Ignatius Moses Setiadi. "Improved Pixel and Bit Confusion-Diffusion based on Mixed Chaos and Hash Operation for Image Encryption", IEEE Access, 2022 Publication	<1 %
18	dergipark.org.tr Internet Source	<1 %
19	inass.org Internet Source	<1 %
20	João Inácio Moreira Bezerra, Vinícius Valduga de Almeida Camargo, Alexandre Molter. "A new efficient permutation-diffusion encryption algorithm based on a chaotic map", Chaos, Solitons & Fractals, 2021 Publication	<1 %
21	De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Rahmawati Zulfiningrum. "Medical image cryptosystem using dynamic	<1 %

josephus sequence and chaotic-hash scrambling", Journal of King Saud University - Computer and Information Sciences, 2022
Publication

22	ebin.pub Internet Source	<1 %
23	eprints.gla.ac.uk Internet Source	<1 %
24	Un Sook Choi, Sung Jin Cho, Jin Gyoung Kim, Sung Won Kang, Han Doo Kim. "Color image encryption based on programmable complemented maximum length cellular automata and generalized 3-D chaotic cat map", Multimedia Tools and Applications, 2020 Publication	<1 %
25	rdoc.univ-sba.dz Internet Source	<1 %
26	Mehmet Demirtas. "AFast Multiple Image Encryption Algorithm Based on Hilbert Curve and Chaotic Map", 2022 Innovations in Intelligent Systems and Applications Conference (ASYU), 2022 Publication	<1 %
27	Yuandi Shi, Rongrong Chen, Donglin Liu, Bin Wang. "A visually secure image encryption scheme based on adaptive block compressed	<1 %

sensing and non-negative matrix factorization", Optics & Laser Technology, 2023
Publication

28	Congxu Zhu, Guojun Wang, Kehui Sun. "Improved Cryptanalysis and Enhancements of an Image Encryption Scheme Using Combined 1D Chaotic Maps", Entropy, 2018 Publication	<1 %
29	Submitted to Shohei High School Student Paper	<1 %
30	Chun-Lai Li, Yang Zhou, Hong-Min Li, Wei Feng, Jian-Rong Du. "Image encryption scheme with bit-level scrambling and multiplication diffusion", Multimedia Tools and Applications, 2021 Publication	<1 %
31	webmail.thescipub.com Internet Source	<1 %
32	www.jport.co Internet Source	<1 %
33	Submitted to Universitas Diponegoro Student Paper	<1 %
34	beei.org Internet Source	<1 %
35	downloads.hindawi.com Internet Source	

		<1%
36	"Applications and Techniques in Information Security", Springer Science and Business Media LLC, 2019 Publication	<1%
37	Hongmin Li, Tie Li, Wei Feng, Jing Zhang, Jun Zhang, Lixia Gan, Chunlai Li. "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion", Journal of Information Security and Applications, 2021 Publication	<1%
38	Submitted to International Islamic University Malaysia Student Paper	<1%
39	ijai.iaescore.com Internet Source	<1%
40	www.aimspress.com Internet Source	<1%
41	Rohan Tuli, Hitesh Narayan Soneji, Prathamesh Churi. "PixAdapt: A novel approach to adaptive image encryption", Chaos, Solitons & Fractals, 2022 Publication	<1%
42	Simiao Wang, Qiqi Peng, Baoxiang Du. "Chaotic color image encryption based on 4D	<1%

chaotic maps and DNA sequence", Optics & Laser Technology, 2022
Publication

43	Xiaoliang Qian, Qi Yang, Qingbo Li, Qian Liu, Yuanyuan Wu, Wei Wang. "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques", IEEE Access, 2021 Publication	<1 %
44	Yuwen Sha, Yinghong Cao, Huizhen Yan, Xinyu Gao, Jun Mou. "An Image Encryption Scheme Based on IAVL Permutation Scheme and DNA Operations", IEEE Access, 2021 Publication	<1 %
45	Zhen Li, Changgen Peng, Weijie Tan, Liangrong Li. "A Novel Chaos-Based Color Image Encryption Scheme Using Bit-Level Permutation", Symmetry, 2020 Publication	<1 %
46	Rui Wang, Guo-Qiang Deng, Xue-Feng Duan. "An image encryption scheme based on double chaotic cyclic shift and Josephus problem", Journal of Information Security and Applications, 2021 Publication	<1 %
47	Vijay Kumar, Ashish Girdhar. "A 2D logistic map and Lorenz-Rossler chaotic system	<1 %

based RGB image encryption approach", Multimedia Tools and Applications, 2020
Publication

---

48 Wei Feng, Jing Zhang. "Cryptanalzing a Novel Hyper-Chaotic Image Encryption Scheme Based on Pixel-Level Filtering and DNA-Level Diffusion", IEEE Access, 2020 <1%
Publication

---

49 Zhao Feixiang, Liu Mingzhe, Wang Kun, Zhang Hong. "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain", Optics & Laser Technology, 2021 <1%
Publication

---

50 Wei Feng, Yigang He, Hongmin Li, Chunlai Li. "A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm", IEEE Access, 2019 <1%
Publication

---

51 Ali K. Mattar, Raad A. Muhajjar, Ali A. Abidali. "Image Blocks Encrypted then Rotated: A New Pixel-Level Scrambling Method Based Logistic Map for IOT", 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), 2022 <1%
Publication

52	Haofu Zheng, Guodong Li, Wenxia Xu, Huiyan Zhong, Xiangliang Xu. "A compressive sensing encryption scheme for dual color images based on discrete memristor map and Rubik's cube scramble", Optik, 2023 Publication	<1 %
53	Lisungu Oteko Tresor, Mbuyu Sumbwanyambe. "A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos", IEEE Access, 2019 Publication	<1 %
54	Sellami Benaissi, Noureddine Chikouche, Rafik Hamza. "A novel image encryption algorithm based on hybrid chaotic maps using a key image", Optik, 2022 Publication	<1 %
55	Shuliang Sun, Yongning Guo, Ruikun Wu. "A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping", IEEE Access, 2019 Publication	<1 %
56	Xingyuan Wang, Xiaohui Du. "Pixel-level and bit-level image encryption method based on Logistic-Chebyshev dynamic coupled map lattices", Chaos, Solitons & Fractals, 2021 Publication	<1 %

57	eprint.iacr.org Internet Source	<1 %
58	netlab.ulusofona.pt Internet Source	<1 %
59	research.riphah.edu.pk Internet Source	<1 %
60	tudr.thapar.edu:8080 Internet Source	<1 %
61	www.nature.com Internet Source	<1 %
62	Yibo Zhao, Ruoyu Meng, Yi Zhang, Qing Yang. "Image encryption algorithm based on a new chaotic system with Rubik's Cube transform and Brownian motion model", Optik, 2022 Publication	<1 %
63	Yibo Zhao, Ruoyu Meng, Yi Zhang, Qing Yang. "Image encryption algorithm based on a new chaotic system with Rubik's cube transform and Brownian motion model", Optik, 2023 Publication	<1 %
64	edoc.gfz-potsdam.de Internet Source	<1 %
65	manuscriptlink-society-file.s3.ap-northeast-1.amazonaws.com Internet Source	<1 %

66	oaji.net Internet Source	<1%
67	www.tandfonline.com Internet Source	<1%
68	Behrouz Vaseghi, Seyedeh Somayeh Hashemi, Saleh Mobayen, Afef Fekih. "Finite Time Chaos Synchronization in Time-Delay Channel and Its Application to Satellite Image Encryption in OFDM Communication Systems", IEEE Access, 2021 Publication	<1%
69	Ajib Susanto, Ibnu Utomo Wahyu Mulyono, Christy Atika Sari, Eko Hari Rachmawanto et al. "Handwritten Javanese script recognition method based 12-layers deep convolutional neural network and data augmentation", IAES International Journal of Artificial Intelligence (IJ-AI), 2023 Publication	<1%
70	Hao Dong, Enjian Bai, Xue-Qin Jiang, Yun Wu. "Color Image Compression-Encryption Using Fractional-Order Hyperchaotic System and DNA Coding", IEEE Access, 2020 Publication	<1%
71	Jianfeng Zhao, Shuying Wang, Litao Zhang. "Block Image Encryption Algorithm Based on	<1%

Novel Chaos and DNA Encoding", Information, 2023
Publication

72 Yongsheng Hu, Han Wu, Luoyu Zhou. "Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion", Alexandria Engineering Journal, 2023 <1%
Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

Combined Interleaved Pattern to Improve Confusion-Diffusion Image Encryption based on Hyperchaotic System

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18