*Iraqi Journal of Science, 2024, Vol. 65, No. 10, pp: 5727-5740*
*DOI: 10.24996/ijs.2024.65.10.33*

**ISSN: 0067-2904**

# Image Encryption Using High-Speed Scrambling and Modular Arithmetic

**Worud M. Saleh*, Mustafa H. Taha, Riyadh J. Mohammad**
*General Directorate of Diyala Education, Diyala , Iraq*

Received: 23/11/2022 Accepted: 28/8/2023 Published: 30/10/2024

**Abstract**

With the enormous growth and advancement of the computer industry, it is critically necessary to transmit a large amount of encrypted multimedia data to prevent third parties from attacking one's privacy or misbehaving. This study proposes a new encryption strategy for preserving original images. It is highly effective and has been shown to be resilient against impulsive noise and loss of data. At first, some random data is entered within the perimeter of the image. Then, three rounds of high-speed scrambling and adaptive diffusion for pixels are carried out to mix the contiguous pixels at random and distribute the newly placed data throughout the image. The suggested encryption method can be used to encrypt original images in any form of representation directly. We offer a particular operation to carry out adaptive diffusion for pixel modulo arithmetic. The results of encryption are evaluated using the histogram, which shows a near-zero correlation with a Number of Pixel Change Rate (NPCR) of 099.624, a Unified Average Change Intensity (UACI) of 033.577, and an average entropy of 7.9993. The proposed method can accomplish much better speed and adapt better to impulse noise and loss of data interference than several conventional and cutting-edge encryption methods.

**Keywords**: Diffusion , Image encryption, Modular arithmetic, NPCR, UACI.

# تشفير الصور باستعمال التخليط عالي السرعة والحساب المعياري

**ورود مهدي صالح, مصطفى حسين طه , رياض جاسم محمد**

المديرية العامة لتربية ديالى، وزارة التربية، ديالى، العراق

**الخلاصة**

مع النمو الهائل والتقدم في صناعة الحاسوب ، من الضروري للغاية نقل كمية من بيانات الوسائط المتعددة المشفرة لمنع الأطراف الثالثة من مهاجمة خصوصية الفرد أو سوء التصرف. تقترح هذه الدراسة استراتيجية تشفير جديدة للحفاظ على الصور الأصلية. الطريقة فعالة للغاية وقد اثبتت أنها مرنة ضد الضوضاء المندفعة وفقدان البيانات. في البداية ، يتم إدخال بعض البيانات العشوائية داخل محيط الصورة. بعد ذلك ، يتم تنفيذ ثلاث جولات ذات سرعة تخليط وانتشار تكيفي للبكسل لمزج وحدات البكسل المتجاورة عشوائيًا وتوزيع البيانات الموضوعة حديثًا في جميع أنحاء الصورة. يمكن استعمال طريقة التشفير المقترحة لتشفير الصور الأصلية بأي شكل من أشكال التمثيل مباشرة. نحن نقدم عملية معينة لتنفيذ الانتشار التكيفي

*Email: hawhra11888@gmail.com

لحساب وحدات البكسل. يتم تقييم نتائج التشفير أثناء استعمال الرسم البياني ، والارتباط شبه الصفري مع عدد معدل تغيير البكسل (NPCR) البالغ 099.624 ، وشدة التغيير الموحد 033.577 (UACI) ، ومتوسط الانتروبيا 7.9993. يمكن للطريقة المصممة خصيصًا تحقيق سرعة أفضل بكثير والتكيف بشكل أفضل مع ضوضاء الاندفاع وفقدان تداخل البيانات مقارنة بالعديد من طرق التشفير التقليدية والمتطورة.

## 1. Introduction

### 1.1 Background

Encryption is the best strategy to deal with the problem of image secrecy, which has arisen recently as a result of advances and developments in the field of technology. Chaotic image encryption is more important in the encryption mechanism due to the unpredictable nature of chaos signals, initial values, and the sensitivity of parameters [1]. The majority of the previous classical cryptographic algorithms, including DES (Data Encryption Standards) and AES (Advanced Encryption Standards), are not applicable anymore in exercises due to the properties that digital images naturally possess, including their huge capacity for data, highly redundant nature, and strong correlation among pixels that are relatively close or adjacent. In light of this, there are a lot of encryption professionals in the field of image ciphering who have recommended brand-new image ciphers according to text ciphers. The chaos theory-based cipher has received a lot of attention [2].

Chaotic systems are frequently and widely used in cryptography because they have highly chaotic features like intense sensitivity to preliminary parameters and conditions and pseudo-randomness [3]. Pixel scrambling consists of the random exchange of all pixels in the spatial domain, with a chaotic nature to the chaos systems. Typically, this approach adjusts pixel positions to undermine the spatial association among pixels in the original plaintext and a pixel inside the encrypted image. Since all chaotic systems have high sensitivity to the initial value and have higher efficiency than the traditional encryption strategy [4], most researchers have designed algorithms to perform the process of encoding images in different formats using all chaos tools [5]. Although all the findings of the researchers employed the idea of chaotic encryption of images with other scientific fields, such as DNA coding [6], algorithms for neural network image ciphering [7], and ciphering of quantum images [8], the basic concept of chaos image encryption is scrambling and diffusion. Modern cryptographic development incorporates cryptographic principles and cryptoanalysis to combat attacks [8] and [9].

Cipher designers make their secret ciphers invulnerable to any known attacks. On the contrary, attackers hack cryptographic systems to try to identify vulnerabilities or weaknesses. Thus, ciphers in cryptography can aid in improving the level of security. In light of the aforementioned research and analyses, we offer a general crypto-analysis technique and correspondingly enhanced algorithm (referred to as Hua's Schema) for digital image encryption. Fundamentally, Hua's scheme consists of pixel insertion at random and two high-speed scrambling rounds with adaptive diffusion for pixels. High-speed scrambling, which adjusts various pixels based on a chaotic system of concatenation, is created to combine neighboring pixels randomly [10].

### 1.2 Related Works

A chaotic-based image cipher was first proposed by the cryptologist Friedrich, who introduced the ciphers for images by using a structure of permutation-diffusion [11]. Particularly, Pak et al. presented an image cipher by using a chaotic sequence that was created according to the differences that were established in the output sequences that have one-

dimensional (1D) chaotic maps [12]. To enhance the protection of the image, the pixels are persuaded to use a DNA scheme, whereas Suri et al. suggested image encryption by intertwining a logistic map and a DNA approach, where the average entropy for a color image is 7.9973 [13]. Some of the flaws have been identified in the existing scheme by Dhall et al. by employing a few numbers of rounds, which have been identified as weak structures and can be easily broken by possessing a small key space [14]. Whereas Abdul et al. used another method for medical image scrambling based on a combination of a linear congruential generator, an exclusive OR shift generator, and a logistic 2D chaotic map for secure transmission [15]. To improve the security, Kumar et al. stated that image encryption with a spiral phase transform along with a chaotic Tinkerbell map for confusion fails to defy entropy attacks [16]. Khan et al. have tested the robustness of the algorithm for various differential attacks and entropy for image encryption based on the Tinkerbell map [17]. Huo et al. stated that by implementing chosen plain text and known plaintext analysis on chaotic cryptosystems, it might reduce the diffusion effect and recover the keystream. They proposed an encryption method for plaintext with two rounds of DNA and a piecewise linear chaotic map for double random phase encoding to generate the ciphertext [18]. For high-speed computation, Dzwonkowski et al. stated a secure image encryption method by quaternion-based lossless with modular arithmetic [19]. Pravees et al. proposed medical image encryption for confidential storage using an improved chaotic economic map by altering sine and cosine functions for multiple rounds [20]. Hua Z et al. stated that medical image encryption involves inserting random data into the surroundings of the image, followed by a logistic sine system for scrambling and diffusion [21]. Liu et al. proposed medical image encryption through a chaotic method for its non-linearity with the use of hyperbolic sine, where metric error analysis has achieved close to ideal values [22]. Zhang has suggested confusion based on piecewise linear chaos and two rounds of diffusion by DNA operations [23]. Enayatifar et al. proposed a system based on DNA sequence operations, Cellular Automata with Tinkerbell Chaos Map for Image Encryption, that withstands various attacks [24]. Chen et al. have reported an efficient image encryption method using DNA encoding and a self-adaptive permutation-diffusion system that uses a hyper-chaotic Lorentz map [22]. Rajput et al. proposed an asymmetric color cryptosystem using polarization-selective diffractive optical elements and a structured phase mask [25]. Huang's scheme, which prevents the recovery of the shuve vectors, thus increasing the security against the chosen plaintext attack, but without a noticeable loss of efficiency [26], offered an encryption technique that used logistic mapping and the combined row and scrambling technique to improve the security characteristics [26]. Guo et al. used the equivalent key attack on the 3D chaotic Baker map-based image cryptosystem. Some of the chaos-based image encryption schemes have been broken [27]. Wu et al. used CTM with a rectangular transform. The scheme included confusion and diffusion, followed by an improved 2D Arnold transform, which thus improved the security of the classical CTM-based method. Wu's algorithm has the advantages of easy design, high encryption speed, and good cryptographic efficiency as far as a typical color image encryption method is concerned. However, it cannot resist the chosen plaintext attack, and the encryption method is insensitive to all secret keys [28].

### 1.3 Contributions

To deal with the problems in existing encryption schemes for protecting plain images, we propose a method to encrypt images with any representation format.

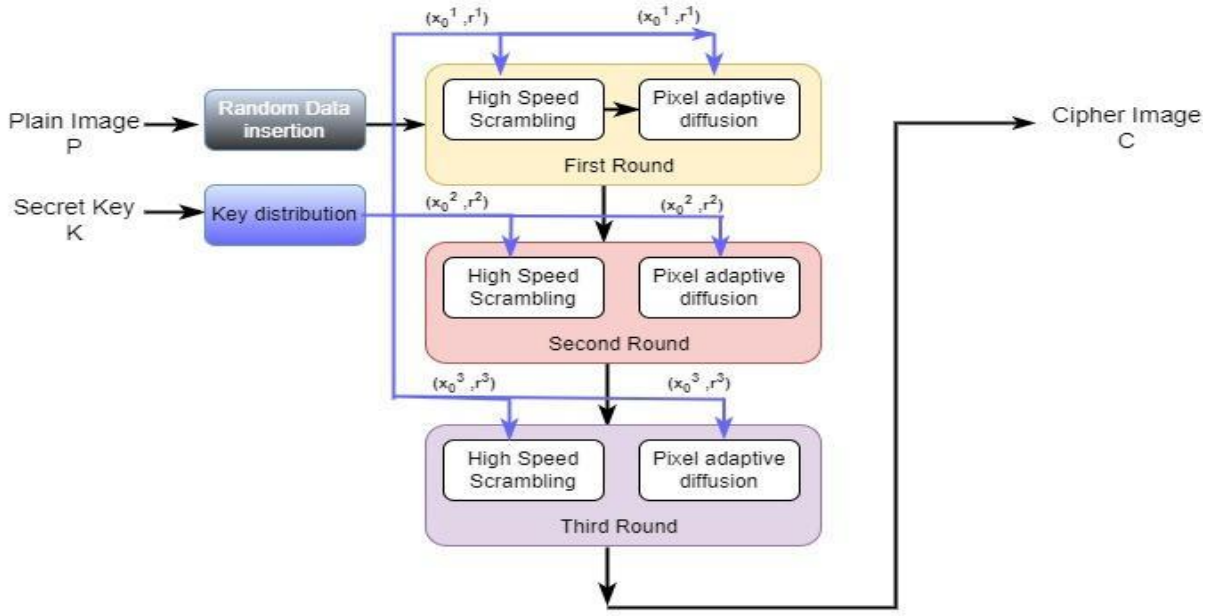
The main contribution of this work is that it can encrypt an identical image into different cipher images, even when using the same secret key based on modulo arithmetic (MA).

Thus, the proposed method provides a protected image with a high level of security and robustness.

The rest of this study is organized as follows: In Section 2, we provide the relevant literature; in Section 3, we present the plain image encryption and decryption systems; in Section 4, we present the simulation results of the proposed encryption scheme and explain its qualities; and in Section 5, the conclusion ends the paper.

## 2. Proposed Scheme of Image Encryption

In this section, we provide a brief, accurate description of the proposed scheme. The scheme is composed of key distribution, random data entry, high-speed scrambling, and pixel adaptive diffusion. Before entering three rounds of permutation-diffusion, the proposed scheme inserts the outermost random pixels into the surrounding plain image. Principal matrices having the same size as the plain image are generated by chaotic systems with different initial states and parameters in the phases of high-speed scramble and adaptive diffusion, consecutively. Bitwise XOR (BX) and modular arithmetic (MA) are applied to diffuse the permuted pixels. The scheme of encryption using BX is named MIE-BX. We pointed out the size of a plain image as (M × N). The structure is displayed in Figure 1, where K is the secret key of length 256 bits. The secret key is decomposed to get sub-keys for diffusion and scrambling during key distribution. The operations of scrambling and diffusion randomize the placements and values of pixels. Inserting random data involves adding some random values to the image's surroundings. Since the encrypted result of each application of our encryption approach is unique, security can be maintained even if the same secure key is used to encrypt the same image many times. To achieve maximum efficiency, our suggested encryption method employs three rounds of encryption to ensure a high level of security. The process of encrypting data is identified as C = Enc. [P, K], while the process of decrypting data is identified as P = Dec. [C, K].




**2.1:** MIE–MA Encryption Algorithm

**Step 1:–**

The secure key K is used to generate pseudo-random numbers for high-speed scrambling and pixel adaptive diffusion. The logistic-sine system (LSS) is used to generate pseudo-random numbers and is denoted as the Logistic Sine System Pseudo Number Generation (LSS-PRNG). It is defined as:

$$X_{n+1} = (rX_n (1 - X_n) + (4 - r) \sin(\pi X_n) / 4) \bmod 1 \quad (1)$$

where the control parameter r ∈ [0, 4] and $X_n$ is the iteration variable and $X_n \in (0, 1)$. Given an initial state ( $X_0$ , r ), a determined pseudo- random sequence { $X_i$ | i = 1 , 2 , ⋯} can be generated. The secure key K is used to generate the initial states for the three rounds of encryption. The variables $x_0$ , r , $R_1$ and $R_2$ are float numbers that can be converted from a 52-bit stream by

$$FN = \sum_{i=1}^{52} Bin_i \times 2^{-i} . \quad (2)$$

Two integers, $d_1$ and $d_2$, can be obtained from a 38-bit stream by

$$IN = \sum_{i=1}^{38} Bin_i \times 2^{i-1} . \quad (3)$$

Then, the initial states for the two encryption rounds can be obtained as follows:

$$\begin{cases} X_0^i = d_i \, x \, (X_0 + R_i) (\mathrm{mod}\ 1) \\ r^i = d_i \, x \, (r + R_i) (\mathrm{mod}\ 4), \end{cases} \quad (4)$$

where i = { 1 , 2, 3 } . Using the initial states ($x_0^1$, $r_1$), ($x_0^2$, $r_2$) and ($x_0^3$, $r_3$), the LSS-PRNG can generate pseudo-random sequences for the three rounds of high-speed scrambling and pixel adaptive diffusion.

**Step2:–**

Suppose the plain-image P is of size M ×N , two random vectors, R of size 2 × N and O of size (M + 2) ×2 , are randomly generated. Their values are represented by the same data format as the pixels of P. The two rows of R are inserted into the top and bottom of P , and the two columns of O are inserted into the left and right of P.

**Step 3:–**

Fast scrambling is achieved by generating a scrambling matrix (S) using chaotic sequences (A of length M & B of length N) with data types and dimensions matching those of the inserted original image. Pixels at coordinates (1, $S_{1,j}$), (2, $S_{2,j}$), and so on have their indexes set to 1, and the column($j$) index is 1. . . . Cells in ( $S_{(1.j)}$ ) are moved upward and joined to form a circle to represent ($M$, $S_{M,J}$) Iterations of the procedure outlined above are carried out until $j$ = N, at which point the desired permuted picture T is obtained.

**Step 4:–**

Diffusion of adaptation for the pixel is the process of spreading a few changes of the original image over the entire pixel range in a cipher image. It is carried out by utilizing the previous pixel and a value that is generated at random to change the content of the current pixel completely. We provide the implementation operation: modulo arithmetic (MA). This is capable of operating at a quick pace in the software environment. The encryption method that was suggested is MA, which is termed MIE–MA. Pixel adaptive diffusion by use of MA as specified:

$$c_{i,j} = \begin{cases} (T_{i,j} \oplus T_{M.N} \oplus Q_{i.j}) \bmod F, & \text{if } i = 1, j = 1, \\ (T_{i,j} \oplus C_{M.(j-1)} \oplus Q_{i.j}) \bmod F, & \text{if } i = 1, j \neq 1, \\ (T_{i,j} \oplus C_{(i-1),j} \oplus Q_{i.j}) \bmod F, & \text{if } i \neq 1. \end{cases} \quad (5)$$

where $\oplus$ denotes the BX operation. Q is a random matrix generated by LSS-PRNG with the initial state ($X_0^i$, $r^i$ ) ( i = 1 in the first round, i = 2 in the second round, and i = 3 in the third round). It has the same size and elements, which represent the same data format pixels in T and i=1, 2,3, … , M ; j=1, 2,3 , … , N.

Iteration: Scrambling and diffusion are to be performed three times in total to arrive at the final cipher output.

### 2.2. MIE–MA decryption algorithm

MIE-MA is symmetric encryption. Hence, the algorithm of decryption in MIE-MA carries out the reverse process. Thus, the steps in decryption are performed in the reverse order of those in encryption.

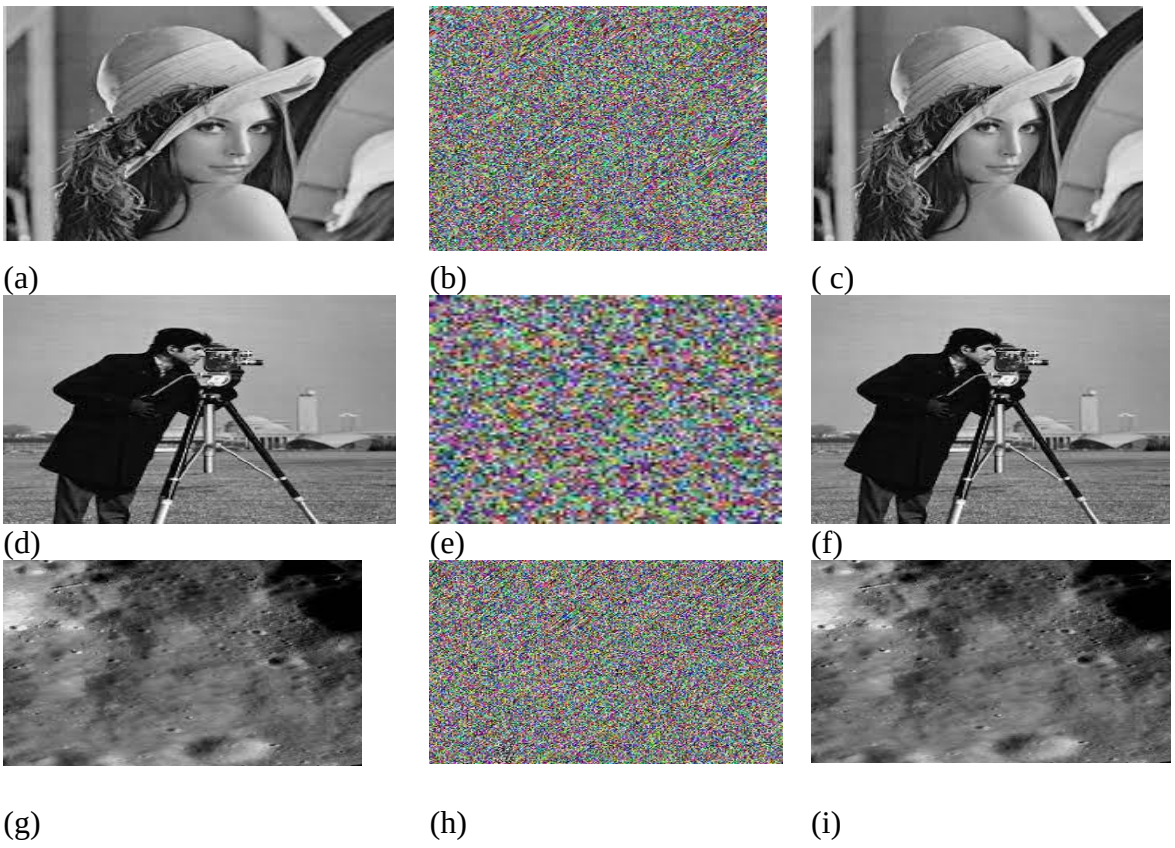
## 3. Security Analysis Based on Simulation Results

To assess the performance and work of IMIE-MA, we evaluate the corresponding simulation security analysis and results.

### 3.1 Simulation Results

The Intel (R) Core$^{TM}$ i7 67000 CPU @ 3.40GHz, 8 GB of RAM, and a Windows 10 desktop PC were used to run the MIE-MA simulation and security analysis shown below. The computer program MATLAB (R2018) was used to carry out MIE-MA. Since MIE-private MA's key is staying the same, the key space is ($2^{256}$), which is large enough to withstand a brute-force attack. We used (4) images and a randomly generated key K=3c94d5b588c45en592n4BA8EF240825CE5E68B6694D6BDCA2D9E1464BD568.

To run simulations. The proposed method has been applied to the images, whose details are shown in Figure 2. From the encoded image output, it is apparent that MIE--MA can convert various original images to cipher images with random distributions. Assailants are unable to use the corresponding cipher images to learn anything about the plain images. By using the right key, MIE-MA may also fully restore the original images to their corresponding cipher images.



(a) (b) ( c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

**Figure 2:** Images Put Through Their Tests With Their Matching Cipher and Decrypted Versions: (a) Lena; (b) Lena's cipher image; (c) Lena's decryption image; (d) Cameraman; (e) Cameraman's cipher image; (f) Cameraman's decryption image; (g) Surface of the Moon (h) Moon Surface Cipher Image (i) Image of the Moon's Surface Encrypted (j) (k) Bird Cryptographic Image (l) Bird Image Decryption3.2. Analysis of Security

### 3.2.1 Analysis of Key Sensitivity

For the ideal high-level security image encryption scheme, both the encryption and decryption processes should produce random outcomes if the secret key is slightly perturbed. Key sensitivity should therefore be evaluated from two perspectives. Though tinkering with the secret keys should generate brand new cipher images, recovering the original ciphertext from the multiple decoded images remains challenging. The expected ratio of variation was 99.5893% at a significance level of 0.05, which was utilized to evaluate the sensitivity of the key. Consequently, the suggested encryption method is very sensitive to a private key if the values of the tested variation ratio are closer to the perfect values.

To evaluate the key sensitivity of MIE-MA in each encryption and decryption process, we randomly generate a 256-bit private key (K). We then randomly changed one bit of K to gain three completely different keys, referred to as (i = 1,..., 3). We then carried out MIE-MA with and on original image P to gain the respective encrypted results C and C i (i = 1, 2,..., 3). At the end, we calculated the differences between C and Ci . For the decryption process, we decrypted C with K and to gain the decrypted images D and (i = 1, 2,..., 3). The difference ratios between D and were then obtained. MIE-MA was similarly tested. All results from the experiment are shown in Table 1. Anyone can notice that the rate and proportions of the difference for the procedures of encryption and decryption are larger than the expected values.

**Table 1:** Analysis of Key Sensitivity (%)

| Keys | Encryption by MIE-MA | Decryption by MIE-MA |
|---|---|---|
| Key (1) | 099.4825 | 99.6732 |
| Key (2) | 099.7487 | 99.7144 |
| Key (3) | 099.4794 | 99.6823 |
| Mean | 099.5702 | 99.6899 |

### 3.2.2 Entropy of Information Analysis

Information entropy is a key measure of randomness that may be applied to the distribution of the gray pixel value. As the distribution of gray values becomes more consistent, the entropy of the image data rises. To compute information entropy (IE), follow these steps:

$$IE(\theta) = -\sum_{i=1}^{256} P(\theta_i) \log_2 P(\theta_i) \quad (6)$$

The probability of an event p(θ) is denoted by the expression p(θi). Since the precise amount of information entropy for grayscale images is 8, attackers will have an extremely hard time deciphering the images. Entropy data for both the original and encrypted versions

of all test images is displayed in Table 2. Each of the cipher images in Table 2 has an almost identical information entropy to (8). Table 3 compares the suggested approach to various newly reported techniques based on the estimated information entropy of a 256-by-256-pixel Lena cipher image.

**Table 2:** Entropy of Information Analysis

| Image | IE | |
|---|---|---|
| | **Plain image** | **Cipher image** |
| **Lena** | 7.5529 | 7.9993 |
| **Cameraman** | 7.1197 | 7.9996 |
| **Moon surface** | 6.8290 | 7.9890 |
| **Bird** | 7.4530 | 7.9996 |
| **Barbara** | 7.5793 | 7.9997 |

**Table 3:** Information Entropy of the Plaintext and Ciphertext Images

| **Image** | **Suggested algorithm** | **Reference**[10] | **Reference**[19] | **Reference**[20] | **Reference**[21] |
|---|---|---|---|---|---|
| **Lena** | **7.9993** | **7.9973** | **7.9978** | **7.9971** | **7.9894** |

### 3.2.3 Analysis of histograms

The gray level histogram of an image, which charts the intensity values L in the interval [0 , L −1] , is a discrete function h ($r_k$ ) = $n_k$ , k = 1 , . . . , L, where $r_k$ is the k th intensity value and $n_k$ is the number of pixels in the image with intensity $r_k$. The histogram of the cipher images is an important characteristic that indicates if the method can resist statistical investigation. It depicts the distribution of pixel values in an image. If the data isn't uniformly distributed, an attacker can glean a certain amount of information through statistical analysis. Because of this, a cipher image with a consistent histogram distribution is required for effective image encryption. A comparison of the unencrypted and encrypted histograms of four test images (Lena, Cameraman, Moon Surface, and bird) is presented in Figure 3. The histograms of the original images were not uniform, but the histograms of the equivalent cipher images were. So, the proposed method may make statistical analysis more difficult.

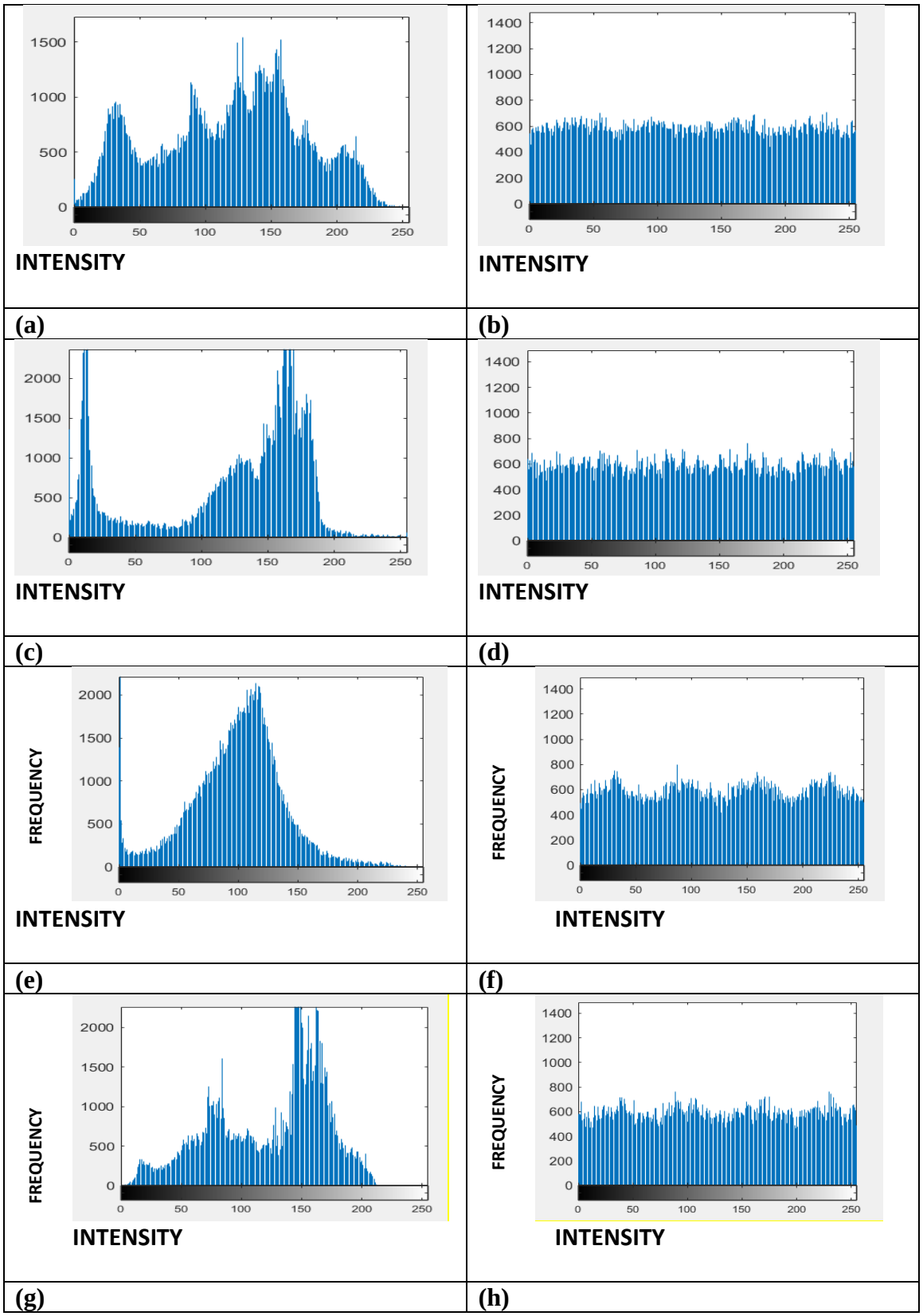



**Figure 3:** Analysis of Histograms (a) Plain Lena's Histogram; (b) Histogram of Cryptographic Ciphers Lena (c) A cameraman's histogram; (d) a cipher cameraman's histogram; (e) a plain moon surface histogram; (f) a surface histogram of the cipher moon; (g) a plain bird histogram; (h) a cipher bird histogram.

$\bar{\mathbf{f}}$: The mean of the histogram has the following formula:

$$\bar{f} = \frac{1}{256} \sum_{\circ=1}^{256} \text{fi} \quad (7)$$

In addition, the formula for determining the standard deviation can be defined as:

$$S = \sqrt{Var} \quad (8)$$

The histogram variance and standard deviation (VAR and S) are displayed in Table 4 for both plain and cipher pictures. Table 4 shows that our approach produces more consistent pixel values in the cipher images.

**Table 4:** Variation and Dispersion in Both Enciphered and Unencrypted Images Are Measured

| Image | Plain | | Cipher | |
|---|---|---|---|---|
| | Var | S | Var | S |
| Lena | 3.4719 x 10 4 | 175.4618 | 273.3561 | 16.7521 |
| Cameraman | 1.1097x 10 5 | 333.1355 | 278.6155 | 17.0124 |
| Moon surface | 1.3409 x 10 5 | 366.2685 | 268.0436 | 16.3721 |
| Bird | 1.2704 x 10 5 | 357.8291 | 216.9531 | 14.7293 |

### 3.2.4 Correlation analysis

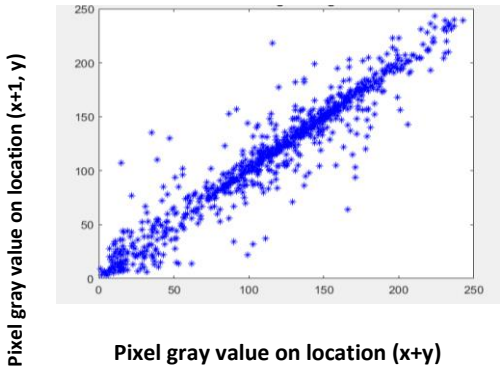
There is often a high degree of connection between neighboring pixels in a plaintext image. Statistical information assaults can be thwarted by decreasing the correlation between neighboring pixels in the cipher text image. This work presents a formula for determining the pixel correlation, and it uses Eqs. (9) and (10) to compute the horizontal, vertical, and oblique correlations between plaintext and cipher text. Figure 4 displays the statistical findings. Table 5 shows that after encryption using this approach, the correlation of the cipher text is near 0, giving it the ability to withstand statistical assaults.

$$r_{x,y} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (9)$$

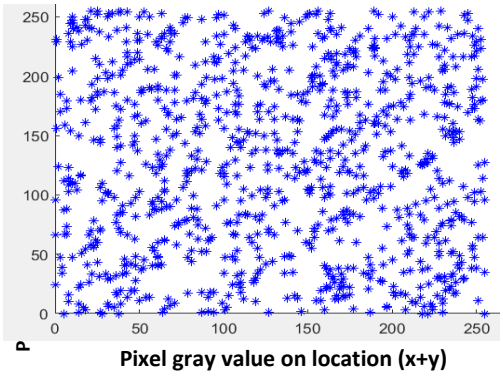
where:

$$\begin{cases} \text{Cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N} \sum_{i+1}^{N} (x_i - E(x))^2 \\ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \end{cases} \quad (10)$$

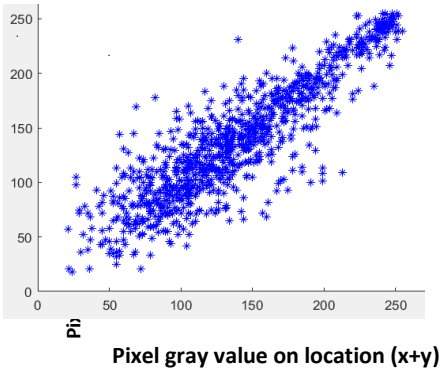
Whereas the selected pixel sequences here are referred to as X and Y, N = 5000 is the whole number of pixels selected from the image, and E(x) and D(x) are the expectation and variance of x, respectively. Figure 4 illustrates the selected pixel sequence distributions in various directions.



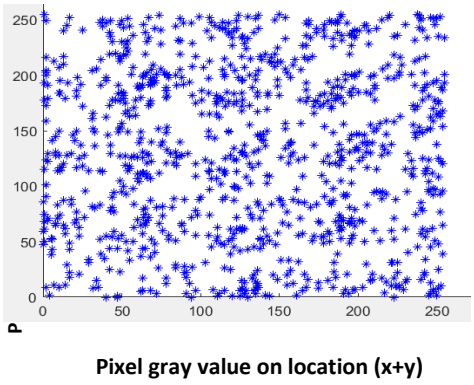

(a) Image of Lena's horizontal correlation



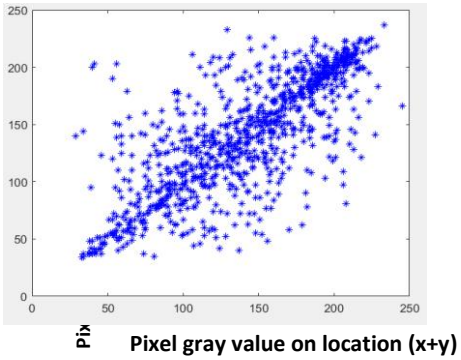

(b) Textual encryption horizontal correlation



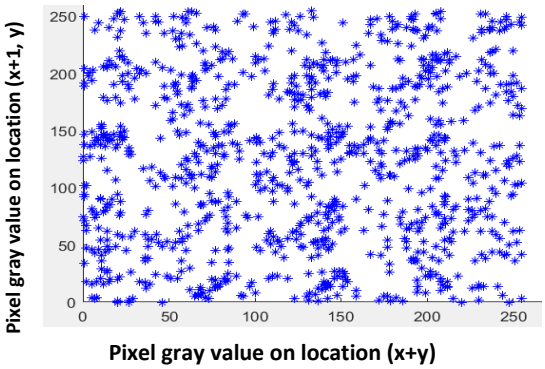

(c) The similarity between Lena's image and the vertical




(d) Vertical correspondence in ciphertext




(e) Lena's image is diagonally related to




(f) Coupling ciphertext in a perpendicular direction

**Figure 4:** Correlation Comparison of Plaintext and Cipher Text

**Table 5:** The Relationship between a Plain Image's Pixels and Their Neighbors in a Cipher Image

| Image | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Lena | 0.9815 | 0.9740 | 0.9314 |
| Cipher text of Lena | -0.0003 | 0.0022 | 0.0974 |
| Bird | 0.9737 | 0.9721 | 0.9988 |
| Cipher text of Bird | -0.0008 | 0.0035 | 0.0014 |
| [19] | 0.0034 | -0.0003 | -0.0011 |
| [22] | 0.0085 | 0.0054 | 0.0049 |
| [9] | 0.0016 | 0.0004 | 0.0300 |

### 3.2.5 Different Analysis

As the sensitivity of the cipher image to the plain picture increases, the algorithm's performance increases against differential assaults. To prevent being cracked by a differential attack, an effective picture encryption technique should make even a tiny change to the plain image, resulting in a noticeable shift in the cipher image. It is usual practice to employ the Number of Pixels Changing Rate (NPCR) and the Unified Average Changing Intensity (UACI) while conducting a differential attack analysis. The ideal ranges for these parameters are NPCR at 99:6094% and UACI at 33:4635%. In this way, they are calculated:

$$UACI=\frac{1}{MXN}\sum_{i=1}^{M}\sum_{i=1}^{N}D(i,j)\ x\ 100\% \quad (11)$$

$$NPCR=\frac{\sum_{i=1}^{M}\sum_{i=1}^{N}|C_1\ (i,j\ )-C_2\ (i,j)|}{MXNX255}\ x\ 100\% \quad (12)$$

*Where*

$$D(i,j)=\begin{cases} 0 & \text{if } C1\ (i,j) = C2(i,j) \\ 1 & \text{otherwise} \end{cases}$$

Here, C1 and C2 are one-pixel-off cipher copies of the original plain image and the updated plain image, respectively. The suggested approach is compared to other previously published algorithms in Table 6. Using the suggested technique, the values of NPCR and UACI were somewhat higher than ideal, indicating that even little modifications to the plain images resulted in vastly different cipher images. Also, using the crucial values of NPCR and UACI [26], we find that the tested cipher images have a random appearance.

**Table 6:** Comparison of Our Algorithm with Newly Published Algorithms Based on Average UACI and NPCR Values

| Algorithm | NPCR % | UACI % |
|---|---|---|
| Proposed algorithm | 099.6246 | 033.5772 |
| Ref.[20] | 099.63 | 033.43 |
| Ref.[26] | 099.613 | 033.466 |
| Ref.[29] | 099.607 | 033.427 |

## 4. Conclusions

This work presents a secure and efficient technique for encrypting images without any further processing. Three components make up this scheme: adaptive diffusion for pixels, high-speed data scrambling, and random data insertion. The goal of random data insertion is to impose a random arrangement on the image's periphery. To randomly reorder neighboring pixels, a high-speed scrambling technique is employed. Pixel values that were added for all pixels will be diffused using an adaptive method. When more bits are utilized to represent each pixel in the picture, the proposed encryption method can run faster, and it can be used instantly for images with any sort of image format. We introduced the proposed encryption method, MIE-MA, which is used to achieve pixel adaptive diffusion via many different processes. They perform exceptionally well in a software environment. Flexibility in execution based on the actual environment is available to all users. MA's high degree of security allows it to outperform many standard encryption methods, providing more efficiency and greater resilience while guarding against data loss and impulsive disturbances. Since our proposed encryption technology is so effective, we plan to investigate its potential application to other types of multimedia data, including videos.

**References**


**[1]** A. A. Abdallah and A. K. Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System," *Iraqi Journal of Science*, vol. 63, no. 1, pp. 324–337, Jan. 2022.

**[2]** N. A. Ali, A. M. S. Rahma, and S. H. Shaker, "3D Content Encryption Using Multi-Level Chaotic Maps," *Iraqi Journal of Science*, vol. 64, no. 5, pp. 2521–2532, May 2023.

**[3]** M. H. Taha and J. M. Al-Tuwaijari, "Improvement of Chacha20 Algorithm based on Tent and Chebyshev Chaotic Maps," *Iraqi Journal of Science*, vol. 62, no. 6, pp. 2029–2039, Jul. 2021.

**[4]** D. Zhang, L. Chen, and T. Li, "Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation," *Entropy*, vol. 23, no. 3, p. 361, 2021.

**[5]** J. A. V. Valencia and B. A. R. Rey, "Phase chaotic encryption and efficiency evaluation for an image multiplexing method," *Opt. Lasers Eng.*, vol. 121, pp. 464–472, 2019.

**[6]** M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

**[7]** P. Mani, R. Rajan, L. Shanmugam, and Y. H. Joo, "Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption," *Inf. Sci. (Ny).*, vol. 491, pp. 74–89, 2019.

**[8]** E. A. Jameel and S. A. Fadhel, "Digital Image Encryption Techniques: Article Review," *Technium*, vol. 4, no. 2, pp. 24–35, Feb. 2022.

**[9]** A. N. Elghandour, A. M. Salah, Y. A. Elmasry, and A. A. Karawia, "An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map," *IEEE Access*, vol. 9, pp. 43411–43421, 2021.

**[10]** A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, pp. 101357–101368, 2021.

**[11]** C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S. M. Qaisar, and K.-Y. Huang, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, p. 2017, 2022.

**[12]** M. Hanif *et al.*, "A novel grayscale image encryption scheme based on the block-level swapping of pixels and the chaotic system," *Sensors*, vol. 22, no. 16, p. 6243, 2022.

**[13]** S. Aashiq Banu and R. Amirtharajan, "Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach," *Multimed. Tools Appl.*, vol. 79, pp. 28807–28824, 2020.

**[14]** Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion," *Opt. Lasers Eng.*, vol. 134, p. 106202, 2020.

**[15]** X. Wang, Y. Su, C. Luo, and C. Wang, "A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling," *PLoS One*, vol. 15, no. 7, p. e0236015, 2020.

**[16]** S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

**[17]** P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map," *Entropy*, vol. 21, no. 7, p. 656, 2019.

**[18]** Q. Sheng, C. Fu, Z. Lin, J. Chen, L. Cao, and C.-W. Sham, "An efficient chaotic image encryption scheme using simultaneous permutation–diffusion operation," *Vis. Comput.*, pp. 1–16, 2023.

**[19]** C. Zhu, Z. Gan, Y. Lu, and X. Chai, "An image encryption algorithm based on 3-D DNA level permutation and substitution scheme," *Multimed. Tools Appl.*, vol. 79, no. 11, pp. 7227–7258, 2020.

**[20]** X.-Y. Wang, J.-J. Zhang, F.-C. Zhang, and G.-H. Cao, "New chaotical image encryption algorithm based on Fisher–Yatess scrambling and DNA coding," *Chinese Phys. B*, vol. 28, no. 4, p. 40504, 2019.

**[21]** T. Li, B. Du, and X. Liang, "Image encryption algorithm based on logistic and two-dimensional lorenz," *IEEE Access*, vol. 8, pp. 13792–13805, 2020.

**[22]** T. Wang and M. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Opt. Laser Technol.*, vol. 132, p. 106355, 2020.

**[23]** M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, pp. 1–13, 2019.

**[24]** R. Zhang et al., "A Novel Plaintext-Related Color Image Encryption Scheme Based on Cellular Neural Network and Chen's Chaotic System," *Symmetry*, vol. 13, no. 3, p. 393, Feb. 2021, doi: 10.3390/sym13030393.

**[25]** X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci. (Ny).*, vol. 486, pp. 340–358, 2019.

**[26]** H. Liu, Y. Zhang, A. Kadir, and Y. Xu, "Image encryption using complex hyper chaotic system by injecting impulse into parameters," *Appl. Math. Comput.*, vol. 360, pp. 83–93, 2019.

**[27]** S. S. Askar, A. A. Karawia, A. Al-Khedhairi, and F. S. Al-Ammar, "An algorithm of image encryption using logistic and two-dimensional chaotic economic maps," *Entropy*, vol. 21, no. 1, p. 44, 2019.

**[28]** H. Huang, S. Yang, and R. Ye, "Efficient symmetric image encryption by using a novel 2D chaotic system," *IET Image Process.*, vol. 14, no. 6, pp. 1157–1163, 2020.