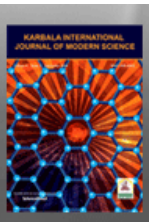

Karbala International Journal of Modern Science

Volume 7 | Issue 3 Article 2

A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation

Ahmed Kareem Shibeeb
Department of Computer Systems, Technical Institute – Suwaira, Middle Technical University, Baghdad, Iraq, ahmed.kareem@mtu.edu.iq

Mohammed Hussein Ahmed
Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq

Ahmed Hashim Mohammed
Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq

Recommended Citation

Shibeeb, Ahmed Kareem; Ahmed, Mohammed Hussein; and Mohammed, Ahmed Hashim (2021) "A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation," *Karbala International Journal of Modern Science*: Vol. 7 : Iss. 3 , Article 2.
Available at: https://doi.org/10.33640/2405-609X.3117

A new chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation

Abstract

In modern chaotic image cryptosystems, the initial values generated for the chaotic system are carried out based on the hash function or summation result of the image pixels. Also, the confusion-diffusion structure is often typically split into two different components. However, it decreases the cryptosystem security because the independent structure can be cryptanalysis separately. A practical chaotic image cryptosystem based on plaintext-associated mechanism and integrated confusion-diffusion operation has been developed in this research paper to enhance the encryption reliability. The initial values of the four-dimensional chaotic system are updated by using the pixel values and locations to increase the sensitivity of plaintext images. Besides, the confusion and diffusion operations are correlated and intertwined with each other, where the proposed scheme applies a simultaneous confusion-diffusion process and rows-columns scrambling process. The simulation and experimental analysis demonstrate that the proposed cryptosystem is protected from possible attacks. Moreover, it provides a high performance compared to several other chaotic-based image cryptosystems.

Keywords

4D chaotic system, Simultaneous confusion-diffusion, Image encryption, Ciphertext difference rate

1. Introduction

Many multimedia data containing sensitive information, including images, videos, and audio signals, are submitted on unsafe public networks such as the internet and mobile networks, which require a powerful cryptographic system to ensure the protection of information. In the past few decades, the protection of sensitive images has gained significant attention from security researchers due to various attacks on transferred data by unauthorized users. Conventional text way cryptographic like DES, AES, Twofish, RSA, etc., are not effective enough to secure digital images because of specific inveterate image properties like bulk data capacity, strong adjacent pixel relationship, and high redundant pixel values [1−3]. Recently, chaotic with high sensitivity to initial conditions, non-periodicity, and strong ergodicity has been commonly used in visual data security applications. There are several desirable features of chaotic-based cryptographic techniques, including sufficient protection and adequate processing time. These techniques involve two operations known as confusion and diffusion operation [4]. In general, the confusion operation is a component of the pixel scrambling. The locations of pixels are replaced randomly without altering the original values of image pixels. However, the diffusion operation focuses on replacing the pixel value with other values to avoid statistical attacks. However, the confusion and diffusion operations have been attacked separately [5]. In the principle of Kerckhoffs, security efficiency must rely only on the confidentiality of the cipher key to make the restoration of the plaintext information almost impossible without the private key [6]. Some attackers perform a type of attack known as chosen plaintext cryptanalysis to decipher the encrypted image without using the cipher key [7]. Hence, the secret key must be associated with the plaintext image information to avoid this dangerous type of attack. On the other hand, some cipher algorithms use summation or average pixel values as secret keys to withstand chosen-plaintext cryptanalysis. However, these algorithms are weak and can be cracked easily [8]. Furthermore, many methods introduce a fast image cryptosystem by avoiding confusion-diffusion architecture.

Based on the above analyses, we notice the following shortcomings in the previous methods:

1. Some cryptosystems utilize the private key without a relationship to the plaintext image, making them weak against chosen-plaintext cryptanalysis.
2. Most plain image-associated cryptosystems depend on pixel values only to generate the secret keys. However, the hacker can easily alter the pixel values or locations of two different pixels to retrieve statistical information.
3. The confusion-diffusion structure is often split into two independent components, allowing the confusion component and diffusion component of the cryptosystem to be cryptanalysis separately.
4. In several schemes, the confusion-diffusion structure is discarded to achieve a faster encryption process.

Abbreviations

4D	Four-dimensional
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Rivest Shamir Adleman
XOR	eXclusive OR
DNA	Deoxyribonucleic Acid
CML	Coupled Map Lattice
S-box	Substitution-box
X^2	Chi-square
CC	Correlation Coefficient
CDR	Cipher-text Difference Rate
CK	Cipher Key
NPCR	Numbers of Changing Pixel Rate
UACI	Unified Averaged Changed Intensity
EQ	Encryption Quality
NIST SP800-22	National Institute of Standards and Technology Special Publication 800−22
GHz	GigaHertz
PC	Personal computer

In this research, we propose an efficient chaotic image cryptosystem based on the four-dimensional chaotic system. It consists of integrated confusion-diffusion operations. Additionally, a new plain image-related function is adopted in the initial values generation. Firstly, the initial states of the chaotic system are updated by extracting the plain image's statistical characteristics, which is highly sensitive to any slight modification in the pixel values and locations of the original image. Based on the produced sequences of the 4D chaotic system, the plain image pixels are scrambled in rows and columns to decrease the correlation between the adjacent pixels.

https://doi.org/10.33640/2405-609X.3117

Then, a simultaneous confusion-diffusion process is applied to the scrambled image to frustrate separate attacks. The latest version of metrics on some standard images is utilized through simulation analysis to evaluate the proposed scheme's efficiency and security. Compared with some previous schemes, these measurement results demonstrate that our proposed method yields preferable security performance and can withstand various attacks. The core novelties of the scheme and its contribution are summarized as follows:

1. We use a new plain text-related mechanism based on the pixel values and locations for initial values generation.
2. The confusion and diffusion operations are integrated, and they intertwine with each other in our cryptosystem.
3. The measurement results demonstrate that the suggested cryptosystem can encrypt various images. Also, it has excellent security efficiency, high performance and can withstand different attacks compared to previous works.

The remainder of this article is structured as follows: The related works are detailed in Section 2. In Section 3, the four-dimensional chaotic system is briefly explained. The operations and steps of the designed image encryption algorithm are illustrated in Sections 4. The simulation results of the current method and its comparison with other existed methods are shown in Sections 5. Finally, Section 6 concludes the whole paper and explains the direction of future research.

2. Related works

Several chaotic image cryptosystems that utilize plaintext image-based key generation have been recently introduced. In Ref. [9], Amina and Mohamed used the output of the hash function of the plaintext image as initial conditions for a modified Logistic-Tent system. The hash function is an authentication scheme used to prove that the received message is the same on the sender side. Amina's method encrypts the gray and medical images based on an independent confusion-diffusion structure. A modified XOR operation governs the bit-level shuffling and circular rotating used for achieving the confusion and diffusion processes. In Ref. [10], Al-Hazaimeh et al. proposed a cryptographic image scheme based on Lorenz chaotic system. The proposed method generates the Lorenz system's initial values and control parameters by using the hash function of the input image. The Lorenz chaotic system is utilized in both the confusion and diffusion processes. Also, Wu et al. [11] generated the controlling parameters and initial states of a coupled map lattice (CML) using the hash function output of the plaintext image. Then, they convert the color image matrices to DNA encoding to apply the bit-level permutation and diffusion operations. Finally, the security of the cryptosystem is improved with pixel-level diffusion. Cao et al. [12] proposed a bit-level image cryptosystem using a two-dimensional Logistic cascade hyperchaotic map. Their scheme uses a bit-level circular shifting to shuffle the pixel's positions and a bit-level XOR reverse procedure to diffuse the pixel's values. Also, they update the initial values of a chaotic map by using ciphertext and cipher key. However, The researchers in Refs. [13,14] avoided the chosen-plaintext cryptanalysis by using the average of the image pixels to produce the keystream of the chaotic map, and do not connect the confusion and diffusion process. Nevertheless, the attacker can easily add one to the encrypted image pixels and substrates one from another or adjust the location of two various pixels to obtain the same average of the plain image. Consequently, the hacker may get a similar output for various input images as shown in Ref. [8], when the researchers exploited chosen-plaintext attack to cryptanalysis a color image cryptosystem based on cellular automata mechanism and hyper-chaotic system that proposed in Ref. [15], despite its used the summation of plaintext image pixels to generate the initial condition of the logistic map. However, the proposed method in Ref. [16] used the secret key without a relationship to the original image. So, it was cracked by chosen-plaintext cryptanalysis and improved to be secure against the possible attacks, as illustrated in Ref. [7]. Mondal et al. [17] suggested a chaotic image cryptosystem based on a chaotic skew tent map and cellular automata. The initial bit sequence of the cellular automata is generated based on the skew tent map without extracting any plain image information. The scrambling operation is performed by using the random output sequence of cellular automata. The chaotic skew tent map is then reused to generate a single random number for the scrambled image diffusion. In Ref. [18], an independent confusion-diffusion structure is developed using a new chaos-based Line map. The proposed system permutes the input image at bit-level, and then it diffuses the scrambled image with XOR operation. The Chen et al. [19] adopted the differential attack to exploit the vulnerable traditional confusion-diffusion structure in Ref. [18]. Opposite, Enayatifar et al. [20] designed an integrated confusion-diffusion structure based on a three-dimensional logistic map and DNA computing to gain a high-efficiency image cryptosystem. However, there is no connection between their system's cipher key and the

Table 1
The comparison results are based on various security parameters.

Schemes	Secret key related to pixels values of the plaintext image	Secret key related to pixels positions of the plaintext image	integrated confusion-diffusion structure	Cracked
Proposed	Yes	Yes	Yes	No
[9]	Yes	No	No	No
[10]	Yes	No	No	No
[11]	Yes	No	No	No
[12]	Yes	No	No	No
[11]	Yes	No	No	No
[12]	Yes	No	No	No
[15]	Yes	No	No	Yes
[16]	No	No	No	Yes
[17]	No	No	No	No
[18]	No	No	No	Yes
[20]	No	No	Yes	No
[21]	Yes	No	No	No
[22]	Yes	No	No	No

original image. Furthermore, Wang et al. [21] introduced a fast, chaotic cryptosystem based on scrambling the columns and rows of the input image. A key encrypts the pixels of rows or columns simultaneously. Their system avoids a chosen-plaintext attack by changing the iteration condition of the logistic map by using the value of the cipher pixels. A similar property of fast image encryption algorithm is proposed in Ref. [22]. Only double chaos-based S-box is applied in two rounds to speed up the encryption process. The proposed algorithm generates the S-box by using a chaotic coupling system based on the Sine-Tent map. It utilizes key sequences associated with the encrypted image to enhance the immunity against chosen plaintext attacks. Table 1 demonstrates the comparison results between the proposed scheme and existed schemes using various security parameters.

3. Four-dimensional chaotic system

It is possible to categorize existing chaotic systems into two types according to the number of dimensions as follows: low-dimensional and high-dimensional systems. The low-dimensional chaotic systems have a simple equation with few variables that provide a low implementation complexity [23,24]. Nevertheless, they have a limited chaotic range which enables them to be predictable [25,26]. In contrast, a wide chaotic range and complicated generators are provided by using high-dimensional chaotic systems [27]. However, their execution time is more significant than those of low-dimensional chaotic systems. In Ref. [28], a four-dimensional chaotic system is proposed with a high chaotic range and low implementation complexity. Thus, the suggested image encryption algorithm will use this chaotic system for chaotic sequence generation. The utilized chaotic system is derived from the Lorenz-Haken model as follow:

$$\begin{cases} \dot{x_1} = \mathrm{a}(x_2 - x_1) \\ \dot{x_2} = -x_2 - bx_3 + (\mathrm{c} - x_4)x_1 \\ \dot{x_3} = \mathrm{b}x_2 - x_3 \\ \dot{x_4} = -dx_4 + x_1x_2 \end{cases} \quad (1)$$

where x_1,x_2,x_3, and x_4 are chaotic system sequences and a, b, c, d are control parameters of the above system. Simulations and analysis results in Ref. [28] had indicated the excellent chaotic behavior that characterizes the 4D system when a = 4, b = 0.5, c = 2, and d ∈ [27,29] regardless of multistability regions of initial condition that determined by SamEn contour plots.

4. The proposed image cryptosystem

The primary operations and steps of the proposed plain image-related cryptosystem are introduced in this section. Firstly, the proposed algorithm adopts the values and positions of an original image to generate the initial values of the four-dimensional chaotic system. Secondly, an efficient and simple rows-column scrambling phase is used to break the relationship among the auto-correlated pixels. Thirdly, the scrambled image is confused and diffused simultaneously, where two traditional phased, confusion and diffusion are integrated into one operation in this cryptosystem. The design of the proposed cryptosystem is explained in Fig. 1.

4.1. Initial values generation

The reliability of a cryptosystem against chosen-plaintext cryptanalysis is one of the most significant

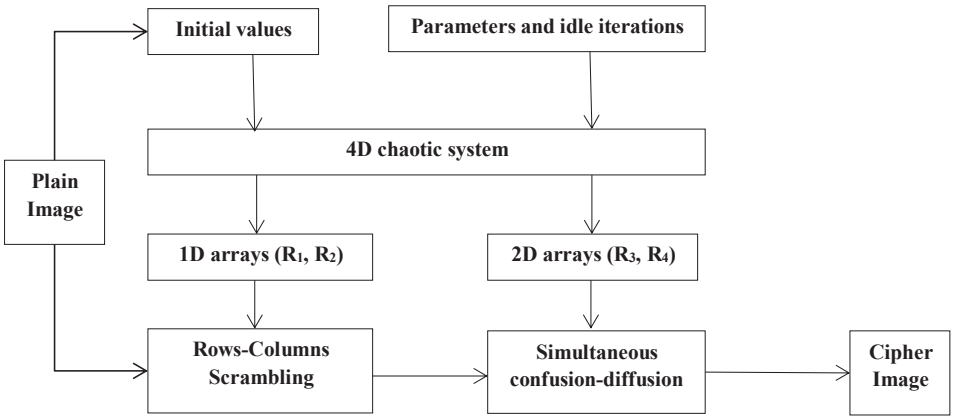

Fig. 1. The flow diagram of the cryptosystem.

problems in digital image security. Many image cryptosystems depend on pixel values only to generate the initial values. However, to retrieve the same average or summation of the plaintext image, the hacker can easily alter two different pixels' pixel values or locations [8,29]. Thus, the initial values for a 4D chaotic system based on the plaintext image are proposed in this work. At first, calculates statistical characteristics (st) by using the pixels values and positions of the original image as follows:

$$st = \sum_{i=0}^{m} \sum_{j=0}^{n} i \times j + O(i,j) \tag{2}$$

Here i and j are the row and column indexes of M × N original image, and $O(i,j)$ is the pixel value. Secondly, influences the initial values of a 4D chaotic system (x_{01},x_{02},x_{03}, and x_{04}) by st as follows:

$$\begin{cases} \dot{x_{01}} = x_{01} + \dfrac{st}{256mn} \\ \dot{x_{02}} = x_{02} + \dfrac{st}{256mn} \\ \dot{x_{03}} = x_{03} + \dfrac{st}{256mn} \\ \dot{x_{04}} = x_{04} + \dfrac{st}{256mn} \end{cases} \tag{3}$$

Then, the initial values $\dot{x_{01}}, \dot{x_{02}}, \dot{x_{03}}$ and $\dot{x_{04}}$ will be modified concerning various plaintext images.

4.2. Rows and columns scrambling

The proposed method uses a rows and columns scrambling operation to completely confuse the plaintext image and disrupt the relationship between neighboring pixels. This operation uses two one-dimensional random arrays based on the output real sequences of a 4D chaotic system, one of which is utilized to scramble the row pixels. The other is used to scramble the column pixels as follows:

$$\begin{cases} i_{new} = Mod\left(\text{Floor}\left(\text{R}_1(i) \times 10^{15}\right), m\right) \\ j_{new} = Mod\left(\text{Floor}\left(\text{R}_2(j) \times 10^{15}\right), n\right) \end{cases} \tag{4}$$

$$S(i,j) = O(i_{new}, j_{new}) \tag{5}$$

where R_1 and R_2 are one-dimensional random arrays generated with the chaotic system. However, Mod (.) and Floor (.) are mathematical functions use to find a remainder of a division and round real number to the nearest integer value, respectively. The output of this phase is scrambled image S(i,j).

4.3. Simultaneous confusion-diffusion

In several schemes, the swap of pixel locations is considered in the permutation phase only. The scrambling operation is entirely independent of the diffusion process. Consequently, it was observed that the two operations above could be attacked independently [30]. A confusion-diffusion operation is applied into a single phase to mixes the current encrypted pixel with the previous one to circumvent this vulnerability. This phase uses two random matrices R_3, R_4 with the same dimensional of pixels as scrambled image S(i,j), then the integrated confusion-diffusion operation can be explained as the below mathematical model:

$$CD(i,j) = \begin{cases} D(i,j) \oplus S(C(i,j)) & IF\ i = 1\ and\ j = 1 \\ CD(i-1,j-1) \oplus D(i,j) \oplus S(C(i,j)) & IF\ i \neq 1\ and\ j \neq 1 \end{cases} \tag{6}$$

$$D(i,j) = Mod\left(\text{Floor}\left(R_3(i,j) \times 10^{15}\right), 256\right) \quad (7)$$

$$C(i,j) = Sort\left(R_4(i,j)\right) \quad (8)$$

where Sort(.) is a mathematical function that returns the index of element location in the matrix after ascending order.

4.4. Encryption process

In this sub-section, the proposed algorithm explains in detail the encryption steps of the suggested scheme. First, the statistical characteristic is extracted from the input image, as illustrated in subsection 4.1. The initial states of the 4D system are updated utilizing st. Then, the proposed algorithm adjusts the position of the pixels in the rows and columns by using the operation of rows and columns scrambling. After that, it implements a simultaneous confusion-diffusion operation on the scrambled image. The essential steps of the encryption process are explained as follows:

Step 1: Input the original image O (i,j) with size M × N, initial conditions (x_{01},x_{02},x_{03}, and x_{04}), system parameters (a, b, c and d) and iterations number (T).

Step 2: Extract the statistical characteristics (st) from the original image by using Equation (2).

Step 3: In Equation (3), the initial conditions of the 4D chaotic system are generated based on st value and input values to avoid known plaintext and chosen plaintext cryptanalysis.

Step 4: Use the updated initial conditions to solve the ordinary equations of the 4D chaotic system with the Euler method. The 4D chaotic system iterates for T + 2 MN times and discard the former T to prevent the transient effect [31]. The remainder chaotic sequences are used to generate four arrays, two of which are one-dimensional (R_1 and R_2). The other is two-dimensional arrays (R_3 and R_4).

Step 5: Use the R_1 and R_2 to scramble the plaintext image pixels in the rows and columns as obtained in Equations (4) and (5).

Step 6: Implement Equations (6)–(8) to confuse and diffuse the pixels of the scrambled image at the same time, and mix the current cipher pixel with the previous one based on the chaotic matrices R_3 and R_4.

With the aforementioned six steps, the encrypted image CD (i,j) is produced. However, the private keys of the suggested scheme consist of idle iterations, updated initial values, and control parameters of a 4D chaotic system, which are utilized to cipher and decipher the input images. The algorithm of the proposed cryptosystem is explained in Algorithm 1.

In the decryption process, the receptor generates the four random arrays (R_1, R_2, R_3, and R_4) based on a 4D chaotic system with the same secret keys. Then, the inverse of simultaneous confusion-diffusion and rows-columns scrambling phases are successfully applied to recover the plain information from the ciphertext image.

Algorithm 1. Encryption process.
Input: Original Image $O_{M\times N}$, Initial conditions x_{01}, x_{02}, x_{03}, and x_{04} , Control parameters a, b, c, and d and Iterations number (T).
Output: Encrypted image$CD_{M\times N}$.
1: Calculate the st value by using Equation (2).
2: Update x_{01}, x_{02}, x_{03}, and x_{04} values by using Equation (3).
3: **for** t = 1 to T+2 × M × N **do**
4: Iterate Equation (2)
5: Generate R_1 of size M;
6: Generate R_2 of size N;
7: Generate R_3 of size M × N;
8: Generate R_4 of size M × N;
9: **end for**
10: C[i,j] = **Sort**(R_3[i,j]);
11: **for** i = 1 to M **do**
12: **for** j = 1 **to N do**
13: i_{new} = **floor** (R_1[i] × 10^{15}) **mod** M;
14: j_{new} = **floor** (R_2[j] × 10^{15}) **mod** N;
15: S[i,j] = O[i_{new}, j_{new}];
16: **end for**
17: **end for**
18: **for** i = 1 to M **do**
19: **for** j = 1 **to N do**
20: D[i,j] = **floor**(R_4[i,j] × 10^{15}) **mod** 256;
21: **if** (i = 1 **&&** j = 1)
22: CD[i,j] = D[i,j] ⊕ S[C[i,j]];
23: **else**
24: CD[i,j] = CD[i,j] ⊕ D[i,j] ⊕ S[C[i,j]];
25: **end if**
26: **end for**
27: **end for**

5. Simulation results

To judge the performance of the suggested cryptosystem, a series of experiments based on the secret key and cipher image was performed. In our experiments,

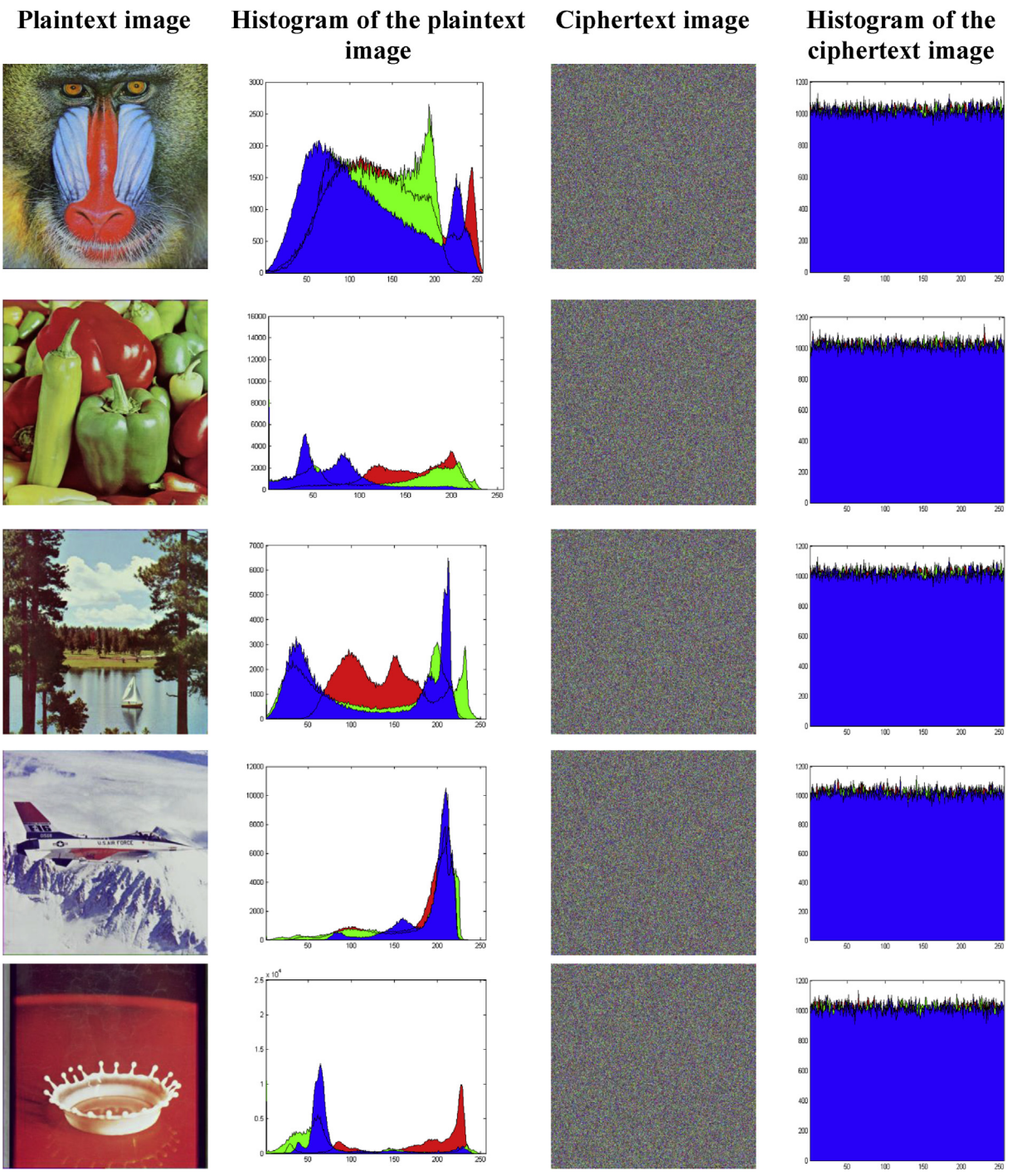

Fig. 2. Color histogram for original images and their encryption result.

Table 2
Quantitative analysis of pixels histogram by X^2.

Image	Baboon	Airplane	Sailboat	Splash	Peppers
Plaintext image	101863.462	822925.960	223807.854	951959.302	340999.441
Ciphertext image	258.844	254.613	252.322	262.118	278.157

the following secret keys were utilized, that is,$x_{01} = 2.0$,$x_{02} = 1.0$,$x_{03} = 1.0$, $x_{04} = 2.0$, a = 4.0, b = 0.5, c = 2.0, d = 27.0 and the number of idle iterations (T) is 650. In the case of the image test, the experiment of the proposed scheme uses various images downloaded from the database of USC-SIPI.

5.1. Statistical cryptanalysis

5.1.1. Histogram metric

The plot of the number of pixels that occur at various intensity values, which are available in the intensity range of 0–255 for an 8-bit image pixel, is referred to as the image histogram. A reliable image encryption algorithm must generate a cipher image with a uniform histogram to resist any statistical cryptanalysis. Fig. 2 shows that the pixel distribution graph of the ciphertext image is even higher than that of the plaintext image. Therefore, the suggested scheme will make cryptanalysis of the image histogram difficult. In addition to the visual result, the distribution of pixels can be justified by a quantitative measure known as chi-square, which is defined by the following mathematical formula [32]:

$$X^2 = \sum_{i=1}^{256} \frac{(P_i - E)}{E} \tag{9}$$

where $P_i$and E are the actual number and the expected number of each gray level value (256) in the tested image, respectively. The encrypted image passes the Chi-square measure if $X^2 < 293.2478$ at significance value $\alpha = 0.05$. Table 2 reflects the success of the proposed image cryptosystem.

5.1.2. Correlation coefficient analysis

The adjacent pixels of a plaintext image are highly related. A cryptosystem must minimize the correlation among neighboring pixels to close to zero [33]. Here, the experiment of the proposed cryptosystem selects 1500 neighboring pairs of pixels randomly for each horizontal, vertical, and diagonal pixel to measure the correlation coefficient of the plaintext and ciphertext image as obtained in the following equations:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{11}$$

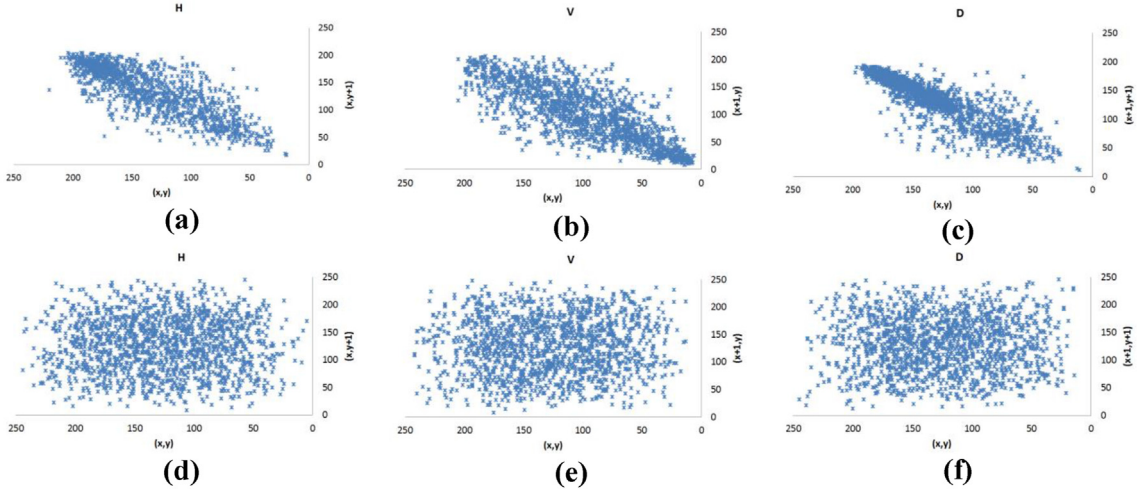

Fig. 3. Adjacent pixels correlation of Peppers image: (a) horizontal correlation of the plaintext image, (b) vertical correlation of the plaintext image, (c) diagonal correlation of the plaintext image, (d) horizontal correlation of the ciphertext image, (e) vertical correlation of the ciphertext image and (f) diagonal correlation of the ciphertext image.

Table 3
The correlation coefficient in various directions.

Image	Plaintext image			Ciphertext image		
	H	V	D	H	V	D
Baboon	0.9832	0.9644	0.9501	0.0013	0.0005	0.0009
Airplane	0.9614	0.9407	0.938	−0.0006	−0.0025	0.0022
Sailboat	0.9482	0.9253	0.9127	0.0007	0.0004	−0.0016
Splash	0.9861	0.9694	0.9373	0.0031	−0.0008	−0.0009
Peppers	0.9694	0.9428	0.9764	0.0004	0.0012	−0.0006

$$CC_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

Here, x_i and y_i denote the gray image values of the neighboring pixels, while the total pixels indicated by N, E(x), and E(y) are the mean values of x_i andy_i. Fig. 3 presents the correlation coefficient values for horizontal, vertical, and diagonal directions.

The numerical results of correlation coefficients of various imagers are shown in Table 3. The result indicates that the correlation coefficients of the encrypted images are very small. These correlation tests indicate that the image cryptosystem close to zero value, meaning that, by using a statistical attack, the hacker cannot extract any useful information.

5.2. Shannon entropy analyses

This measurement can be utilized to define the randomness of pixels in a tested image. Global Shannon entropy for 256 gray levels can be defined as follows:

$$E(w) = \sum_{i=1}^{M} \mathrm{P}(z_i)\log_2 \mathrm{P}(z_i) \tag{13}$$

where $\mathrm{P}(z_i)$ stands for the probability of message z_i and M is the total value of z_i. For a random ciphertext message, the optimal value of global Shannon entropy is 8. Wu et al. used local Shannon entropy over randomly selected f non-overlapping image blocks with fixed number of pixels (T_b) to overcome inaccuracy, inconsistency, and low efficiency problems in traditional entropy [34]. The local Shannon entropy is defined as:

Table 4
Global entropy and local entropy tests at f = 30, T_b = 1936 and a = 0.001.

Image	Baboon	Airplane	Sailboat	Splash	Peppers
Global entropy	7.9986	7.9994	7.9991	7.9981	7.9993
Local entropy	7.9626	7.9719	7.9811	7.9924	7.9731

$$\overline{E_{k,T_b}}(w) = \frac{1}{f}\sum_{i=1}^{f} E(w_i) \tag{14}$$

where $E(w_i)$ is the traditional entropy of image blocks w_i and f is the number of non-overlapping image blocks. For a good image cryptosystem, the $\overline{E_{k,T_b}}(w) \in [7.9015,\ 7.9034]$ at $f = 30$ and $T_b = 1936$ and confidence parameter a = 0.001. As reported in Table 4, the local entropy values of the ciphertext image fall into an ideal interval that protects the output image of the proposed scheme against different statistical attacks.

5.3. Key space and key sensitivity

The secret key space is the size of the total of all variables utilized in the cryptosystem. To avoid brute-force cryptanalysis, the secret key space must be greater than 2^{100} [35]. For our proposed image cryptosystem, the secret keys are comprised of the initial statesx_{01},x_{02},x_{03}, and x_{04}, the system parameters a, b, c, d, and idle iteration T. Using the double-precision IEEE-754 standard, each initial state and system parameter of the 4D system will take 10^{-15} [36]. The idle iteration is integer number T ∈ [500,1000]. Consequently, the total key size of the proposed method is around $(10^{15})^8 \times 500 \approx 2^{409}$, which is obviously more than 2^{100}, rendering brute-force attacks impossible.

One common procedure for checking the sensitivities of these secret key is to decipher the encrypted image with a tiny key modification utilizing ΔCK (i.e. changing x_{01} tox_{01} + ΔCK or x_{01} − ΔCK). Then, the proposed scheme uses a cipher-text difference rate (CDR) test to verify the difference between the decrypted images and the original one in the proposed image cryptographic scheme. This measure can be obtained by the following equations [37]:

$$Diff(I_1(i,j), I_2(i,j)) = \begin{cases} 0\ IF\ I_1(i,j) = I_2(i,j) \\ 1\ IF\ I_1(i,j) \neq I_2(i,j) \end{cases} \tag{15}$$

$$Diff_{sum}(I_1, I_2) = \sum_{ij} Diff(I_1(i,j), I_2(i,j)) \tag{16}$$

$$CDR = \sum_{ij} \frac{Diff_{sum}(CI_1, CI_2) + Diff_{sum}(CI_1, CI_3)}{2 \times M \times N} \times 100\% \tag{17}$$

where $I_1(i,j)$and $I_2(i,j)$ referred to the encrypted the pixel values before and after key changing; CI_1, CI_2 and $CI_3$are cipher images using different encryption keys CK, CK + ΔK, and CK −ΔCK, respectively. In general,

Table 5
Cipher-text difference rate (CDR) analysis of Peppers image for different secret keys CK with $\Delta CK = 10^{-15}$ for initial conditions and control parameters and $\Delta CK = 10^{0}$ for idle iterations.

Modified CK	CK value	CDR%
X_{01}	2.0	99.6023
X_{02}	1.0	99.611
X_{03}	1.0	99.6047
X_{04}	2.0	99.5789
a	4.0	99.6217
b	0.5	99.5143
c	2.0	99.6073
d	27.0	99.6256
T	650	99.6305

having a CDR of more than 99% is considered a sufficient key sensitivity for an encryption scheme. To calculate CDR for the proposed scheme, the proposed algorithm modify the entire secret key with a tiny change + ΔCK and −ΔCK on the Mandrill image as explained in Table 5. According to the obtained results, it can be observed that the proposed scheme provides a higher value of CDR. Hence; the proposed scheme performs well in the CDR measure.

5.4. Resistance to differential attack

Some attackers attempt to modify the cryptosystem input image and measure the effect in the output image (that is, an encrypted image of the plaintext and the ciphertext image of plaintext with a small modification). The operation which aids to attack a cryptosystem is called differential attack; where the attacker measures the correlation between the input image and the two output images. The Numbers of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) are the two significant tests utilized for this attack. These tests can be computed as follows:

$$V(i,j) = \begin{cases} 0 \; IF \; CI_1(i,j) = CI_2(i,j) \\ 1 \; IF \; CI_1(i,j) \neq CI_2(i,j) \end{cases} \tag{18}$$

$$NPCR = \sum_{ij} \frac{V(i,j)}{M \times N} \times 100\% \tag{19}$$

$$UACI = \sum_{ij} \frac{|CI_1(i,j) - CI_2(i,j)|}{255 \times M \times N} \tag{20}$$

where $CI_1(i,j)$ and $CI_2(i,j)$ are the two ciphertext images referring to the plaintext image before and after a small modification; M and N determine the image length and width, respectively. The ideal case of NPCR and UACI tests count on the images size and significance level α according to obtained results in Ref. [38], where the 512 × 512 gray image pass all theoretical NPCR critical values at any significance level if the result of $NPCR \geq 99.5893\%$, and it pass the UACI test if the result within the critical interval of (33.3730%, 33.5541%), (33.3445%, 33.5826%) and (33.3115%, 33.6156%) at significance level ($\alpha = 0.05$), ($\alpha = 0.01$) and ($\alpha = 0.001$), respectively. The results in Tables 6

Table 6
Results of the NPCR measure.

Images	NPCR%	The Critical value of NPCR		
		$NPCR^*_{0.05} = 99.5893\%$	$NPCR^*_{0.01} = 99.581\%$	$NPCR^*_{0.001} = 99.5717\%$
Baboon	99.6251	Succeed	Succeed	Succeed
Airplane	99.7014	Succeed	Succeed	Succeed
Sailboat	99.7293	Succeed	Succeed	Succeed
Splash	99.748	Succeed	Succeed	Succeed
Peppers	99.6941	Succeed	Succeed	Succeed

Table 7
Results of the UACI measure.

Images	UACI	The Critical value of UACI		
		$UACI^-_{0.05} = 33.373$ $UACI^+_{0.05} = 33.5541$	$UACI^-_{0.01} = 33.3445$ $UACI^+_{0.01} = 33.5826$	$UACI^-_{0.001} = 33.3115$ $UACI^+_{0.001} = 33.6156$
Baboon	33.4631	Succeed	Succeed	Succeed
Airplane	33.3794	Succeed	Succeed	Succeed
Sailboat	33.4827	Succeed	Succeed	Succeed
Splash	33.5144	Succeed	Succeed	Succeed
Peppers	33.4248	Succeed	Succeed	Succeed

Table 8
The results of the EQ test.

Image	Baboon	Airplane	Sailboat	Splash	Peppers
EQ	775.4286	794.1388	686.9752	791.242	786.5531

and 7 show that the suggested scheme can provide a robust encryption process.

5.5. Encryption quality

The encryption operation alters the pixel values from what they were before encryption. High-level modifications in pixel values improve the quality of the encryption process; hence the encryption quality (EQ) represents the aggregate modifications in pixel values among the plaintext and ciphertext images. The EQ measure is computed as follows [39]:

$$EQ = \sum_{q=0}^{2^8-1} \frac{(\mathrm{Hq(OI)} - \mathrm{Hq(CI)})^2}{2^8} \tag{21}$$

where Hq(OI) and Hq(CI) are the number of occurrences for each gray level q in the plaintext and ciphertext images, respectively. Increasing encryption equality to a higher degree is an important matter for the secure image cryptosystem. Table 8 presents the results of the EQ test for various images, from which we can see that the EQ of our cryptosystem is satisfactory.

5.6. NIST random number experiments

In general, the NIST SP800-22 experiments are utilized for testing the randomness quality of the cryptosystem and pseudo-random generator. In this article, the proposed cryptosystem evaluates the randomness of the encrypted image. However, the pseudo-random generator has been evaluated in Ref. [28]. This metric includes fifteen sub statistical tests and takes sequences of bits as input. All of the subtests produce a p-value within an interval (0, 1). To put the cryptosystem in possession of the required randomness properties, the produced p-value should be more significant than 0.01 [3]. Table 9 illustrates NIST tests of an encrypted version of the Peppers image, which can be shown that the suggested cryptosystem produces a ciphertext image that passes all randomness metrics.

Table 9
Randomness results of encrypted Peppers image using NIST-800-22 metrics.

NIST experiment	P-value	Succeed/Failed
Frequency (monobit)	0.931172	Succeed
Block-frequency (Len. = 128)	0.425546	Succeed
Cumulative-sums (Reverse mode)	0.218267	Succeed
Runs	0.348340	Succeed
Longest-run	0.617253	Succeed
Serial (Len. = 16)	0.915842	Succeed
Non-overlapping templates (Len. = 9)	0.655731	Succeed
Discrete Fourier transform	0.823116	Succeed
Maurer's “universal statistical”	0.226447	Succeed
Approximate entropy (Len. = 10)	0.642851	Succeed
Overlapping templates (Len. = 9)	0.088632	Succeed
Random-excursions (X = 1)	0.057663	Succeed
Random-excursions variant(X = −1)	0.392470	Succeed
Linear-complexity (Len. = 500)	0.297486	Succeed
Binary matrix rank	0.313762	Succeed

5.7. Computational time analysis

The cryptosystem running time is a substantial requirement for real-time applications. The simulation runs on a laptop with Intel Core (i3-2328M) 2.20 GHz CPU, 4 GB RAM. The OS and computational platforms are Windows 7 64 bit and Visual studio C#.net 2015, respectively. The average time of the encryption/decryption compute by the scheme for image processing with different sizes 256 × 256, 512 × 512, and 1024 × 1024 is 0.0982 s, 0.3927 s, and 0.5236 s respectively. According to these results, the proposed model has a suitable speed for real-time image encryption applications.

5.8. Performance comparison with previous schemes

In this section, the proposed method's performance is compared with existing schemes in Refs. [7,9,12,15,17,21,22]. Table 10 presents the dominance of Chi-square, correlation coefficient, global Shannon entropy, key space, NPCR, and UACI of our method on Peppers image with the size of 512 × 512 compared to the previous methods. The use of integrated confusion and diffusion operations and the use of plaintext image information for the initial states of the 4D chaotic method are the main reason for the dominance of the proposed method.

In speed analysis comparison, this article measures the rate of cycles per byte and megabytes per second to provide a fair judge on the performance of cryptosystems. The higher the Megabytes per second are, the more the encrypted bytes get processed in second. In contrast, the cycles per byte test mean the number of cycles required to encrypt one byte. The smaller number of these tests indicates the lower computational load needed for the cryptosystem [40]. Table 11 has compared the results of speed analysis of the proposed scheme with existing cryptosystems. It can

Table 10
Comparison of our cryptosystem with some of the existing cryptosystems using Peppers image.

Schemes	X^2	Correlation			Global Entropy	Key-space	NPCR%	UACI
		H	V	D				
Proposed	278.157	0.0004	0.0012	−0.0006	7.9993	$\approx 2^{409}$	99.6941	33.4248
[7]	252	−0.0242	0.0137	−0.0169	7.9993	$\approx 2^{138}$	99.6128	33.5513
[9]	276.79	0.0115	0.0109	−0.0101	7.9993	$\approx 2^{384}$	99.6315	33.6315 (**Failed**)
[12]	254.896	0.0003	0.0014	0.0007	7.9993	$\approx 2^{221}$	–	–
[15]	–	−0.0052	−0.0002	0.0005	7.9973	$\approx 2^{300}$	99.6254	33.4566
[17]	–	−0.0263	0.0015	0.0126	7.9998	$\approx 2^{256}$	99.6937	30.8424 (**Failed**)
[20]	–	0.0053	0.0138	0.0019	7.9983	$\approx 2^{240}$	99.3017 (**Failed**)	33.0026 (**Failed**)
[21]	–	–	–	–	7.9973	$\approx 2^{90}$	99.61	33.23 (**Failed**)
[22]	–	–	–	–	7.9975	$\approx 2^{258}$	–	–

Table 11
The speed analysis comparison results.

Schemes	Image type	Image size	Encryption time (Unit: s)	PC speed (Unit: GHz)	Megabytes per second	Cycles per byte
Proposed	RGB	512 × 512	0.3927	2.20	1.9099	1099
[9]	Gray	512 × 512	0.139	3.0	1.7986	1591
[12]	Gray	256 × 256	0.3243	1.9	0.1927	9403
[17]	RGB	512 × 512	3.1037	2.20	0.2416	8684
[18]	RGB	512 × 512	3.161	3.1	0.2373	12,458
[20]	Gray	256 × 256	0.281	2.3	0.2224	9863
[21]	Gray	256 × 256	0.0652	2.20	0.9586	2189
[22]	Gray	512 × 512	1.708	3.3	0.1463	21,511

be illustrated that our scheme has excellent security efficiency, high performance, and can resist recent attacks compared to previous cryptosystems.

6. Conclusion

This research article has developed a new image encryption scheme based on a plaintext-associated mechanism and integrated confusion-diffusion architecture. Unlike the traditional image encryption method, the suggested method updates the initial conditions of the 4D chaotic system based on the pixel values and positions of the original image to enhance the plaintext sensitivity property. We then used the produced sequence of a 4D chaotic system to decrease the correlation among the neighboring pixels by shuffling them in the rows and columns based on the operation of rows and columns scrambling. After that, we implement a simultaneous confusion-diffusion structure on the scrambled image to avoid the independent attack. Besides, the simultaneous confusion-diffusion operation achieves high security by mixing the current encrypted pixel with the previous one. The proposed scheme applies in simulation framework and evaluates the security and performance through the latest version of measurements like Chi-square, correlation coefficient, global and local Shannon entropy, key space, CDR, encryption quality, NPCR, UACI, and computational time analysis. Compared to existing systems, these results illustrate that our system has high reliability, low computational time, and can withstand recent attacks. On the other hand, the proposed cryptosystem does not evaluate against noise and occlusion attacks. Thus, in our future study, we will exploit the computing efficiency and high security of the proposed method to encryption of visual sensors image in wireless multimedia sensor networks. . Moreover, it also involves testing the immunity of our system against noise and occlusion attacks.

References

[1] A. Arab, M.J. Rostami, B. Ghavami, An image encryption method based on chaos system and AES algorithm, J. Supercomput. 75 (2019) 6663–6682, https://doi.org/10.1007/s11227-019-02878-7.

[2] A. Malik, S. Gupta, S. Dhall, Analysis of traditional and modern image encryption algorithms under realistic ambience,

Multimed, Tools Appl. 79 (2020) 27941–27993, https://doi.org/10.1007/s11042-020-09279-6.
[3] S.M. Kareem, A.M.S. Rahma, A novel approach for the development of the Twofish algorithm based on multi-level key space, J Inf Secur Appl. 50 (2020) 102410, https://doi.org/10.1016/j.jisa.2019.102410.
[4] A. Alghafis, N. Munir, M. Khan, An encryption scheme based on chaotic Rabinovich-Fabrikant system and S 8 confusion component, Multimed Tool Appl. 80 (2021) 7967–7985, https://doi.org/10.1007/s11042-020-10142-x.
[5] E.Y. Xie, C. Li, S. Yu, J. Lü, On the cryptanalysis of Fridrich's chaotic image encryption scheme, Signal Process. 132 (2017) 150–154, https://doi.org/10.1016/j.sigpro.2016.10.002.
[6] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S.W. Baik, A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image, Multimed Tool Appl. 75 (2016) 14867–14893, https://doi.org/10.1007/s11042-015-2671-9.
[7] J. Chen, F. Han, W. Qian, Y.D. Yao, Z. liang Zhu, Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map, Nonlinear Dynam. 93 (2018) 2399–2413, https://doi.org/10.1007/s11071-018-4332-9.
[8] M. Li, D. Lu, W. Wen, H. Ren, Y. Zhang, Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata, IEEE Access. 6 (2018) 47102–47111, https://doi.org/10.1109/ACCESS.2018.2867111.
[9] S. Amina, F.K. Mohamed, An efficient and secure chaotic cipher algorithm for image content preservation, Commun Nonlinear Sci Numer Simulat. 60 (2018) 12–32, https://doi.org/10.1016/j.cnsns.2017.12.017.
[10] O.M.A. Mohammad, F.A.N. Alhindawi, Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys, Neural Comput. Appl. 31 (2017) 2395–2405, https://doi.org/10.1007/s00521-017-3195-1.
[11] X. Wu, K. Wang, X. Wang, H. Kan, J. Kurths, Color image DNA encryption using NCA map-based CML and one-time keys, Signal Process. 148 (2018) 272–287, https://doi.org/10.1016/j.sigpro.2018.02.028.
[12] C. Cao, K. Sun, W. Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Process. 143 (2018) 122–133, https://doi.org/10.1016/j.sigpro.2017.08.020.
[13] L. Liu, S. Miao, A new simple one-dimensional chaotic map and its application for image encryption, Multimed Tool Appl. 77 (2018) 21445–21462, https://doi.org/10.1007/s11042-017-5594-9.
[14] J. Tang, Z. Yu, L. Liu, A delay coupling method to reduce the dynamical degradation of digital chaotic maps and its application for image encryption, Multimed Tool Appl. 78 (2019) 24765–24788, https://doi.org/10.1007/s11042-019-7602-8.
[15] A.Y. Niyat, M.H. Moattar, M.N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Opt Laser Eng. 90 (2017) 225–237, https://doi.org/10.1016/j.optlaseng.2016.10.019.
[16] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Process. 138 (2017) 129–137, https://doi.org/10.1016/j.sigpro.2017.03.011.
[17] B. Mondal, S. Singh, P. Kumar, A secure image encryption scheme based on cellular automata and chaotic skew tent map, J Inf Secur Appl. 45 (2019) 117–130, https://doi.org/10.1016/j.jisa.2019.01.010.
[18] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, Q. Liu, A novel image encryption algorithm based on chaos and Line map, Neurocomputing. 169 (2015) 150–157, https://doi.org/10.1016/j.neucom.2014.11.095.
[19] L. Chen, B. Ma, X. Zhao, S. Wang, Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map, Nonlinear Dynam. 87 (2017) 1797–1807, https://doi.org/10.1007/s11071-016-3153-y.
[20] R. Enayatifar, A.H. Abdullah, I.F. Isnin, A. Altameem, M. Lee, Image encryption using a synchronous permutation-diffusion technique, Opt Laser Eng. 90 (2017) 146–154, https://doi.org/10.1016/j.optlaseng.2016.10.006.
[21] X. Wang, Q. Wang, Y. Zhang, A fast image algorithm based on rows and columns switch, Nonlinear Dynam. 79 (2015) 1141–1149, https://doi.org/10.1007/s11071-014-1729-y.
[22] S. Zhu, G. Wang, C. Zhu, A secure and fast image encryption scheme based on double chaotic S-boxes, Entropy. 21 (2019) 790, https://doi.org/10.3390/e21080790.
[23] S. Pan, J. Wei, S. Hu, A novel image encryption algorithm based on hybrid chaotic mapping and intelligent learning in financial security system, Multimed Tool Appl. 79 (2020) 9163–9176, https://doi.org/10.1007/s11042-018-7144-5.
[24] K. Suneja, S. Dua, M. Dua, A review of chaos based image encryption, in: 2019 3rd Int. Conf. Comput. Methodol. Commun., IEEE, 2019, pp. 693–698, https://doi.org/10.1109/ICCMC.2019.8819860.
[25] C. Li, T. Xie, Q. Liu, G. Cheng, Cryptanalyzing image encryption using chaotic logistic map, Nonlinear Dynam. 78 (2014) 1545–1551, https://doi.org/10.1007/s11071-014-1533-8.
[26] J. Chen, F. Han, W. Qian, Y.-D. Yao, Z. Zhu, Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map, Nonlinear Dynam. 93 (2018) 2399–2413, https://doi.org/10.1007/s11071-018-4332-9.
[27] S.A. Mehdi, S.J. Muhamed, Design and analysis of a novel six-dimensional hyper chaotic system, Al-Mustansiriyah J Sci. 31 (2020) 62–71, https://doi.org/10.23851/mjs.v31i4.901.
[28] H. Natiq, M.R.M. Said, N.M.G. Al-Saidi, A. Kilicman, Dynamics and complexity of a new 4d chaotic laser system, Entropy. 21 (2019) 34, https://doi.org/10.3390/e21010034.
[29] C. Li, Y. Zhang, E.Y. Xie, When an attacker meets a cipher-image in 2018: a year in review, J Inf Secur Appl. 48 (2019) 102361, https://doi.org/10.1016/j.jisa.2019.102361.
[30] H. Wen, S. Yu, Cryptanalysis of an image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps, Eur Phys J Plus. 134 (2019) 1–16, https://doi.org/10.1140/epjp/i2019-12797-4.
[31] Z. Bashir, N. Iqbal, M. Hanif, A novel gray scale image encryption scheme based on pixels' swapping operations, Multimed Tool Appl. 80 (2021) 1029–1054, https://doi.org/10.1140/epjp/i2019-12797-4.
[32] A.S. Mahmood, M.S.M. Rahim, Novel method for image security system based on improved SCAN method and pixel rotation technique, J Inf Secur Appl. 42 (2018) 57–70, https://doi.org/10.1016/j.jisa.2018.08.001.
[33] M.H. Ahmed, A.K. Shibeeb, F.H. Abbood, An efficient confusion-diffusion structure for image encryption using plain image related Henon map, Int. J. Comput. 19 (2020) 464–473, https://doi.org/10.47839/ijc.19.3.1895.
[34] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, Inf. Sci. (Ny). 222 (2013) 323–342, https://doi.org/10.1016/j.ins.2012.07.049.
[35] S.A. Banday, M.K. Pandit, A.R. Khan, Securing medical images via a texture and chaotic key framework, in: Multimed.

Secur., Springer, 2021, pp. 3−24, https://doi.org/10.1007/978-981-15-8711-5_1.

[36] E. Yavuz, A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme, Opt Laser. Technol. 114 (2019) 224−239, https://doi.org/10.1016/j.optlastec.2019.01.043.

[37] E. Yavuz, R. Yazıcı, M.C. Kasapbaşı, E. Yamaç, A chaos-based image encryption algorithm with simple logical functions, Comput. Electr. Eng. 54 (2016) 471−483, https://doi.org/10.1016/j.compeleceng.2015.11.008.

[38] Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption, Cyb J Multidiscip J Sci Technol J Sel Areas Telecommun. 1 (2011) 31−38.

[39] H. Movafegh, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Process. 164 (2019) 163−185, https://doi.org/10.1016/j.sigpro.2019.06.010.

[40] Z. Qiao, S. El Assad, I. Taralova, Design of secure cryptosystem based on chaotic components and AES S-Box, AEU - Int J Electron Commun. 121 (2020) 153205, https://doi.org/10.1016/j.aeue.2020.153205.