ITC 1/50

Information Technology and Control
Vol. 50 / No. 1 / 2021
pp. 55-75
DOI 10.5755/j01.itc.50.1.28012

A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing

Received 2020/11/14 | Accepted after revision 2020/12/17

http://dx.doi.org/10.5755/j01.itc.50.1.28012

HOW TO CITE: SundaraKrishnan, K., Jaison, B., Raja, J. P. (2021). A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing. *Information Technology and Control,* 50(1), 55-75. https://doi.org/10.5755/j01.itc.50.1.28012

A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing

K. SundaraKrishnan

Department of Computer Science and Engineering; Alagappa Chettiyar Government College of Engineering and Technology; Karaikudi, Tamilnadu, India; phone: +917708795039; e-mail sundarakrishnank@gmail.com

B. Jaison

Department of Computer Science and Engineering; RMK Engineering College; Chennai Tamilnadu, India; phone: +919840024357; e-mail: bjn.cse@rmkec.ac.in

S. P. Raja

Department of Computer Science and Engineering; Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology; Chennai, Tamilnadu, India; phone: +919486181212; e-mail: avemariaraja@gmail.com

Corresponding author: sundarakrishnank@gmail.com

The transmission of sensitive and secret images over a public network demands effective techniques to safeguard and conceal the data. In this paper, a symmetric multiple color image encryption technique is proposed by adopting a dual permutation and dual substitution framework. Initially, the input images are combined into a large image and then segmented into pure-image elements. These pure-image elements are permuted using the elementary cellular automata Rule-30 and zigzag pattern scanning. Finally, pixel values are substituted by employing the circular shift method and 2D logistic map. The efficiency of this method is quantified, based on the unified average changing intensity (UACI), information entropy, number of pixels change rate (NPCR), key sensitivity, key space, histogram, peak signal-to-noise ratio (PSNR) and correlation coefficient (CC) performance metrics. The outcome of the experiments and a comparative analysis with two similar methods indicate that the proposed method produced high security results.

KEYWORDS: Cellular automata; chaos; substitution; permutation; mixed image elements.

1. Introduction

High speed networks and communication infrastructure in the modern digital facilitate easy and rapid online communication. Online, real-time communication is put to good use in telemedicine, weather monitoring, defense surveillance, and social media, to name a few. In these fields, images area primary source of information and, further, a massive quantum of visual content is transmitted using public networks and stored in the cloud. Given that such digital images may contain secret and sensitive information of a personal, financial or national nature, it is imperative to ensure their safety in order to stop in formation leaks. Image encryption is a great way to protect digital images, especially during their transmission. Image encryption renders meaningful images unrecognizable. Classical encryption techniques that work well on textual data do not do so on images, owing to their high correlation and colossal dimensions. Therefore, digital image enciphering has emerged as a key area of study. Over the last few years, experts have proposed image ciphers based on the chaos theory and cellular automata. Cellular automata exhibit fascinating properties like complex behavior and unpredictability in terms of simple rules, while chaotic maps possess excellent sensitivity and ergodicity. Hence, the union of cellular automata (CA) and chaos theory-based image encryption design offers a superior solution for image security issues.

1.1. Related Work

Wolfram introduced the notion of using cellular automata to produce secret keys [34], and since then much work has been carried out on CA-based ciphers. Jin proposed a fast image cipher using a cellular automata-generated attractor as the encryption function [12]. In this technique, the state attractor based key streams contain at most eight states only. Zhang et al. [41], proposed a two-dimensional cellular automata-based image cryptosystem, in which balanced CA are used for permutation. The experiments proved that this technique powerful enough to withstand statistical attacks. Chai et al. proposed an image encryption and compression technique by employing CA and compressive sampling [5]. Their algorithm uses the cellular automata rule to achieve confusion. But the entropy values of the encrypted images are low. Jeyaram [11] et al. proposed a new cellular automata-based image cipher that uses a radius-2, class-III CA to scramble pixels. A cellular automata and DNA computing-based image encryption method was presented by Zhou et al. [45]. Their scheme introduces the Thymine DNA cellular automata and T-DNA-CA for encryption. This algorithm has high computational overhead. Mondal et al. proposed a cellular automata-based image cryptosystem [19], where CA are adopted to produce a pseudo-random sequence that confronts noise attacks efficiently. Hanis [9] et al. presented a dual-image encryption-compression technique that employs cellular automata and a modified convolution technique. Their scheme utilized a set of CA rules to scramble pixel locations. Perales [21] proposed a cellular automata-based color image cipher, with the elementary CA Rule-45 used for key generation. Asadollahi et al. [2], proposed an image enciphering method based on cellular automata and the Arnold map, wherein cellular automata are used to change pixel values. The above schemes are designed only for single-image encryption.

Matthews [18] pointed to the application of chaos in encryption algorithms, and since then a slew of chaos theory-based image ciphers have been presented. An image encryption fusion and compression approach, based on chaos and compressive sampling, was put forward [17], with a 1D logistic map used to build a sensing matrix. Ramasamy [22] et al. introduced an image cipher using enhanced logistic-tend map. This scheme achieved both confusion and diffusion properties of an ideal cipher. A novel image cryptosystem that uses a 1D logistic map and random sampling was introduced by Zhu et al. [46]. The hardware and software design of 1D map-based schemes are simple, but the smaller key space makes the technique susceptible to brute force attacks. The RGB image cipher, using chaos and the Chinese remainder theorem, was introduced by Guo et al. [8]. Their technique uses a chaotic quantum map to shuffle the RGB image. Patro [20] et al. proposed a chaos theory-based multi-image cryptosystem whereas cross-coupled map is used for executing diffusion and permutation operations, with the results indicating that their algorithm confronts known plain-image and chosen plain-image attacks. Sui et al. [25], presented a dual image enciphering scheme using a logistic map and the discrete fractional transform. The logistic map in this technique relocates and modifies image pixel values, and the method demonstrates a significant resistance to conventional cipher image-only attacks. Sui et al. again presented a dual-image cipher using a fractional angular transform and coupled logistic map [26], wherein the fractional computation takes a much longer encryption time. Liu [16] et al. proposed a chaotic system-based dual-image cryptosystem employing S-boxes and a chaotic sequence for dual-image diffusion, with a large key space being the strength of the algorithm. Zhang [40] et al. presented a chaotic map and a permutation model-based multiple-image cipher technique. Li et al. [14], proposed a dual-image enciphering scheme by adopting the chaos theory and gyrator transform, in which a standard map is utilized to generate the position of the pixel scrambling area. A cycle shift and chaos theory-based image cipher was proposed by Wang et al. [33], where pixel substitution is realized by the circular shift which greatly increases security. Zhou et al. designed a 1D logistic map and co-sparse representation-based dual-image encryption scheme [44], utilizing the chaotic map to construct a measurement matrix. This method showed poor resistance against statistical attacks. Tutueva [29] et al. introduced a method using adaptive chaotic map to construct chaos-based cipher. This scheme achieved larger key space. Tutueva [30] et al. again utilized adaptive chatic maps to create hash function. This novel approach effectively counters birthday attack.

Sawlikar [24] et al. reported a dual-image encryption and compression scheme that undertakes two stages of encryption for enhanced security strength. Alfalou et al. [1], introduced a many-image simultaneous encryption, fusion and compression scheme in which encryption is executed by utilizing biometric information. A multiple-image cipher to protect medical images was proposed [3]. Zhong [42] et al. presented a dual-image cryptosystem by adopting random-phase encoding. Zhang [37] et al. designed a many-image cipher scheme utilizing the orthogonal basis matrix and double random-phase encoding, where images are encrypted in parallel. Their algorithm strongly resists occlusion attacks, though the computation cost is higher. Xiong [36], proposed a vector decomposition-based many-image cryptosystem that uses private keys, in addition, for enhanced security. Chen [6] et al. presented a multiple-image asymmetric cipher based on compressive sampling and feature fusion. In reference [43], Nanrun et al. developed a dual-image enciphering technique using the discrete fractional random transform and discrete wavelet transform. Zhang [39] et al. introduced a novel many-image encryption scheme based on the mixed-image elements obtained from the many images used. Xiaoqiang et al. [38], again designed a multi-image cipher using chaos and mixed-image content. Karawia [13] et al. developed a many-image cryptosystem based on an economic map and mixed-image elements. Most of the dual- and multi-image ciphers presented above are indented only for grayscale image encryption.

1.2. Motivation and Justification

An array of internet-based applications, such as telemedicine, cloud computing, and social media, transmit large volumes of secret images over public networks. The security of these sensitive images is a major concern, with image encryption working best for image data protection. Cellular automata are very simple rules that generate highly complex random patterns that have been applied successfully in cryptographic algorithms. Chaos is a phenomenon that occurs in greatly sensitive, deterministic nonlinear dynamical systems. It is extremely difficult to predict chaos behavior, and chaos theory has been a good candidate for image encryption techniques. Circular shift operations can be used to perform value substitution operations effectively and with little computation, while zigzag order scanning can be used for satisfactory permutation operations. Reconstructing an original image from very small-sized, mixed-image elements is impossible without keys. All of the above has motivated the development of a symmetric color image encryption scheme using cellular automata, zigzag scanning, circular shifts, chaos and mixed-image elements. The proposed algorithm obtains good numerical results, thus demonstrating that the new scheme is most suitable for multiple color image encryptions.

1.3. An Outline of the Proposed Work

The proposed technique consists of the following five main steps: a) secret keys are calculated from input images; b) the input images are combined into a large image and pure- image elements obtained by segmentation; c) two-level permutation is performed using cellular automata and zigzag scanning; d) two-level substitution is performed using the circular shift and 2D-logistic map, and e) the big encrypted image is segmented into smaller images.

1.4. Contribution

The contributions of our work include the following: a) Dual permutation – dual substitution framework: image encryption is performed by adopting a dual permutation and dual substitution framework that effectively dissipate the statistical structure of plaintext and enhances confusion property; b) Key Selection: The initial configurations for cellular automata, the starting position for zigzag scanning, the starting seeds for the logistic map, and the 512-bit hash are the keys of this system which offers larger key space and withstand plaintext-based threats.

1.5. Paper Organization

The rest of this paper is arranged as follows. Section 2 describes the mixed-image elements, cellular automata, zigzag pattern, circular shift and 2D logistic map. Section 3 presents the proposed multiple color image enciphering and deciphering procedures. Section 4 outlines the experimental setup. Section 5 lists and analyzes, in detail, the experimental results. Section 6 discusses the results, and Section 7 concludes the paper.

2. A Basic Background

2.1. Mixed Image Elements

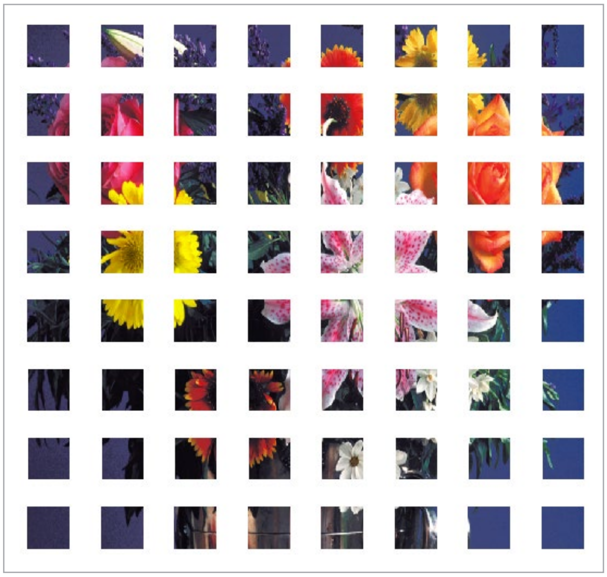
Matrix algebra makes it possible to segment a matrix into sub-matrices and, conversely, sub-matrices can be combined to form a single matrix. Images are treated as matrices while processing so they can be divided and merged [38-39]. For instance, the input image1, shown in Figure 1.a, can be segmented into 64 small sub-images, as shown in Figure 1.b, and the sub-images joined easily. Consider that P^1_{mxn} P^2_{mxn},...., P^h_{mxn} are h original plain images divided into the sub-image sets, $S^1=\{s^1_i\}$, $S^2=\{s^2_i\}$,..., $S^h=\{s^h_i\}$. Each member of the set $s_i \in S$ is called a pure-image element. A new mixed set,

Figure 1.a

Flowers Image

Figure 1.b

Pure image elements of flowers image



X = $\{\{s_i^1\} \cup \{s_i^2\} \cup ... \cup \{s_i^h\}\}$, can be created from mixing the pure elements. Each member of the set, $x_i \in X$, is termed a mixed-image element

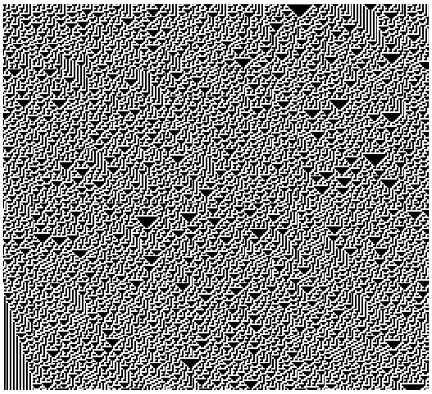
2.2. Cellular Automata

Conventional science uses mathematical models to describe phenomena in the natural world. The underlying principle of cellular automata (CA) is the use of simple rules, in the form of programs, to create models that describe the world [34]. What is remarkable about cellular automata is that very simple rules produce extremely intricate random patterns as they evolve over time. More generally, CA is an array of discrete cells, wherein every cell is colored either black (1) or white (0). The content (color) of every cell it contains is updated parallelly at each step in its evolution, based on simple definite rules. The CA rule sets produce four classes of patterns: nesting, randomness, repetition and complex [33]. We are motivated to use the random class pattern in the design of our cipher. Elementary cellular automata (ECA) are a basic form of cellular automata in which the state of each cell depends on only three cells. The new state of a cell is defined by Equation (1),

$$k_j^{t+1} = g(k_{j-1}^t, k_j^t, k_{j+1}^t), \tag{1}$$

Where k_j^{t-1}, k_j^t and k_j^{t+1} represent the state of cell j at time t-1, t and t+1, respectively, and g is the function that represents the rule. The rule used in this scheme is Rule-30 from the ECA, which states that every cell must be looked at in relation to the cell at its right. If the color of both cells was white in the previous step, the new color of the cell must be the same as the previous color of the cell to its left – or else, the new color must be the opposite [34]. Figure 2.a shows Rule-30 and Figure 2.b how differently Rule-30 behaves from its random initial state (condition). The finite cellular automaton is employed in the proposed scheme, in which cells are arranged in a ring structure where the right neighbor of the rightmost cell is the leftmost cell, and the left neighbor of the leftmost cell is the rightmost cell [12].

Figure 2.b
Example of an evolution of rule-30



2.3. Zigzag Patterns

The zigzag pattern used in this work carries out second-level pixel permutation to enhance the strength of the cipher. This is done by scanning the matrix in the zigzag manner shown in Figure 3.a, while transforming the matrix representation of the image into a one-dimensional vector. In a zigzag scanning pattern, the starting point is salient, since different starting points produce different permutation orders. For instance, the matrix shown in Figure 3.b is scanned from two different starting points and the results shown in Figure 3.c and Figure 3.d. The starting point of the zigzag scanning pattern is obtained from the

Figure 2.a
The mapping of the rule-30

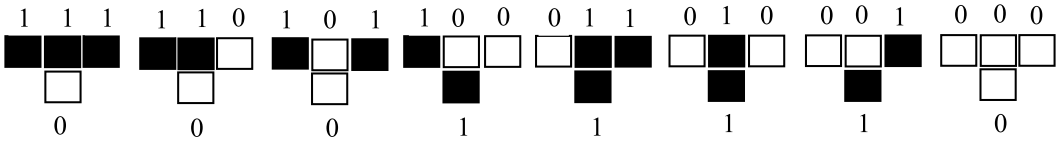
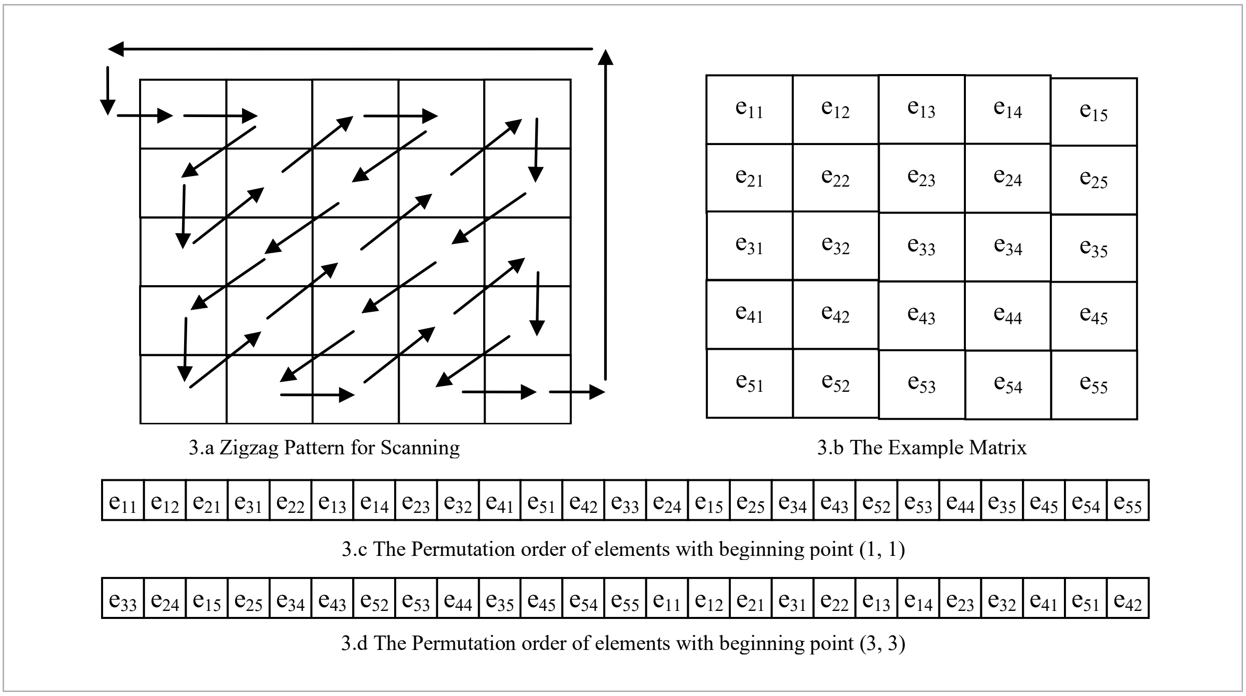


Figure 3
Example of Zigzag Scanning



3.a Zigzag Pattern for Scanning

e_{11}	e_{12}	e_{13}	e_{14}	e_{15}
e_{21}	e_{22}	e_{23}	e_{24}	e_{25}
e_{31}	e_{32}	e_{33}	e_{34}	e_{35}
e_{41}	e_{42}	e_{43}	e_{44}	e_{45}
e_{51}	e_{52}	e_{53}	e_{54}	e_{55}

3.b The Example Matrix

e_{11}	e_{12}	e_{21}	e_{31}	e_{22}	e_{13}	e_{14}	e_{23}	e_{32}	e_{41}	e_{51}	e_{42}	e_{33}	e_{24}	e_{15}	e_{25}	e_{34}	e_{43}	e_{52}	e_{53}	e_{44}	e_{35}	e_{45}	e_{54}	e_{55}

3.c The Permutation order of elements with beginning point (1, 1)

e_{33}	e_{24}	e_{15}	e_{25}	e_{34}	e_{43}	e_{52}	e_{53}	e_{44}	e_{35}	e_{45}	e_{54}	e_{55}	e_{11}	e_{12}	e_{21}	e_{31}	e_{22}	e_{13}	e_{14}	e_{23}	e_{32}	e_{41}	e_{51}	e_{42}

3.d The Permutation order of elements with beginning point (3, 3)

input images so that every new input image has a different zigzag pattern. This input dependency of the algorithm resists chosen plaintext-based attacks.

2.4. Circular Shift Operations

Circular shift operations, which are reversible, change pixel values simply and efficiently [33]. There are two types of circular shift operations, left and right. In a k-bit left circular shift, each bit is shifted a k binary digit to the left, circularly. Consider an n-bit binary sequence, $B_n = \{b_0,b_1 ...b_{n-2}, b_{n-1}$, where $0\leq n \leq n-1\}$. The 1-bit left circular shift operation changes the binary sequence as follows:$\{b_1, b_2... b_{n-1}, b_0\}$. For instance, if a four-bit sequence $(1000)_2$ is circularly shifted 1-bit left, the result is $(0001)_{2,}$ that is, the decimal $(8)_{10}$ is changed to the decimal $(1)_{10}$. The k-bit left circular shift is employed in the proposed system to perform the first-level pixel value substitution.

2.5. The Two-Dimensional Logistic Chaotic Map

Chaos is a complex behavior, arising from a deterministic nonlinear dynamical system that exhibits the two special properties of unpredictability and sensitivity. It is hard to predict chaos behavior, and a system like this one is highly sensitive to the starting seeds. These two properties make the chaos theory most suited to developing ciphers. The 2D logistic map [32] used in the proposed system is defined in Equation (2). It has a best distribution than provided by previously proposed logistic maps.

$$k_j^{t+1} = g(k_{j-1}^t, k_j^t, k_{j+1}^t\ ), \tag{2}$$

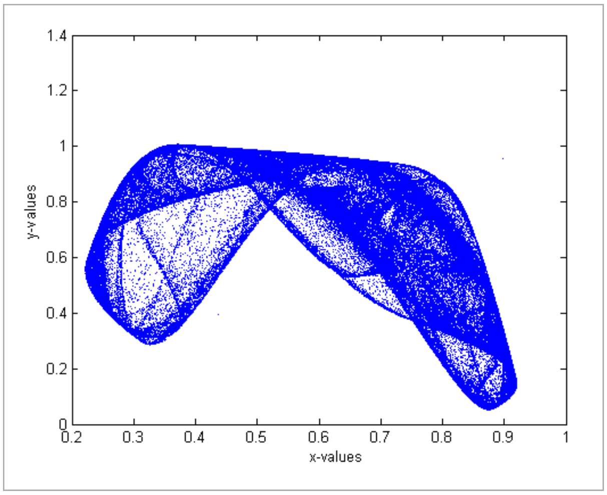
where p_1, p_2, q_1 and q_2 are parameters. The 2D logistic map behaves chaotically when the value of the parameters ranges between $2.75 < p_1 \leq 3.4$, $2.7 < p_2 \leq 3.45$, $0.15 < q_1 \leq 0.21$ and $0.13 < q_2 \leq 0.15$. The trajectory of the 2D logistic map for the parameters (p_1=2.98, p_2=3.30, q_1=0.18, q_2=0.15) and starting values (x_1=0.898 and y_1=0.954) is shown in Figure 4.

Bifurcation Diagram

Bifurcation phenomenon displays the change in dynamic behavior when the control parameters change to a critical point [28, 31]. Bifurcation diagrams of the Equation (2) are shown in Figure 5. The fixed point and period-doubling are observed from the bifurcation di-

Figure 4

Trajectory of the 2-D logistic map



agram. It is clear from the Figure 5 that Equation (2) turns into chaos through double periodic bifurcation.

Lyapunov Exponent

Lyapunov exponent is a standard way to measure the degree of sensitive dependence on initial seeds of dynamical systems [27]. The Largest Lyapunov Exponent is nonnegative in the chaotic region [9]. The Lyapunov exponents for the Equation (2) is calculated [23] for the time series and the initial seeds of the Equation (2) as: (x_1 = 0.898 and y_1 = 0.954). It can be observed form the Figure 6 that the positive Lyapunov exponent contribute to the support of hyper chaotic.

Figure 6

Largest Lyapunov Exponent

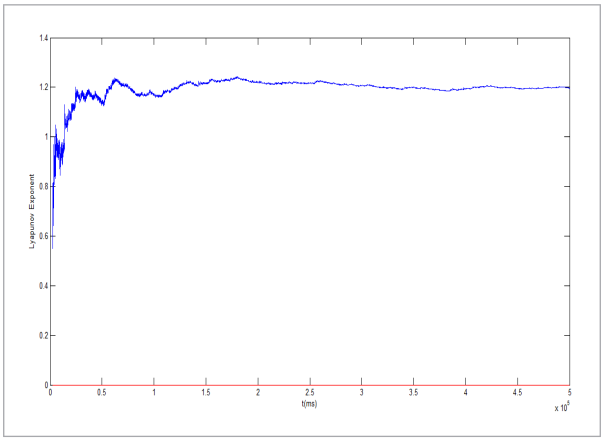
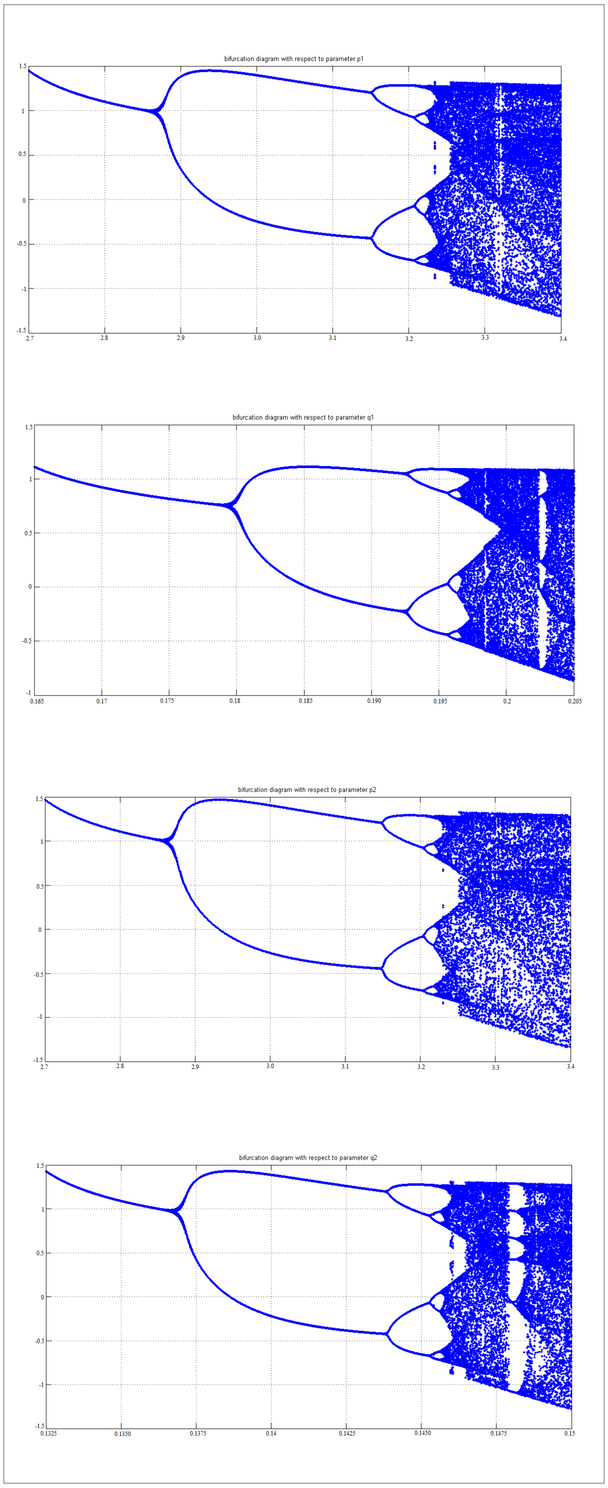


Figure 5

Bifurcation Diagram with respect to parameters (p1, p2, q1 and q2)



3. The Proposed Algorithm

The framework of the new system is shown in Figure 7. The two prime and inevitable cipher design principles of confusion and diffusion are realized in this approach through the inclusion of substitution and permutation operations. The key generation, enciphering and deciphering processes are explained here.

3.1. Key Generation

The initial configurations for cellular automata, the starting position for zigzag scanning, the starting values for the logistic map, and the 512-bit hash are the keys of this system. To withstand plaintext-based threats, the keys are computed from the input images and obtained as follows:

Step 1: Obtain the 512-bit hash by applying the SHA-512algorithm on the input images.

Step 2: Compute the initial configuration.

The two initial configuration vectors, $\{R_0^p \text{ and } C_0^p\}$, for Rule-30 are calculated from the 512-bit hash as follows.

Case 1: If the length of configuration (L) is 1≤ L ≤512, select L bits from the rear end of the 512-bit hash in reverse order.

Case 2: If the length of configuration (L) is ≤1024, select the first 512 bits from the rear end of the 512-bit hash in reverse order and the remaining bits from the front end in the forward order.

Step 3: Find the starting position of the zigzag scanning pattern.

The 512-bit hash of the input image is grouped into 8-bit segments and transformed to 64-decimal numbers, d_1, d_2, d_3, ..., d_{64}. The starting position ($p_{0,}$ q_0) of the zigzag scanning pattern is computed using Equation (3),

$$\begin{cases} p_0 = ((d_1 + d_{64}) \bmod w) + 1 \\ q_0 = ((d_2 + d_{63}) \bmod w) + 1' \end{cases} \qquad (3)$$

where w is the dimension of the image.

Step 4: Compute the starting values of the 2D logistic map.

In the 2D logistic map, the two initial values (x_1, y_1) used are computed using Equation (4),

$$\begin{cases} x_1 = \dfrac{1}{2}(\mathrm{mod}\,((d_1 \oplus d_2 \oplus \ldots . . \oplus d_{32}), 256) + x_s) \\ y_1 = \dfrac{1}{2}(\mathrm{mod}\,((d_{33} \oplus d_{34} \oplus \ldots . . \oplus d_{64}), 256) + y_s) \end{cases} . \qquad (4)$$

where (x_s, y_s) are the starting seeds.

3.2. Encryption Algorithm

Figure 8 shows the flowchart of the proposed multiple color image encryption process. The process of transforming h plain images into h encrypted images consists of the following steps.

Step 1: Combine all the h input images to create one large image (I).

Step 2: Create pure-image elements by segmenting the large image.

Step 3: Generate the mixed-image elements. A per-

Figure7

Block diagram of the proposed technique

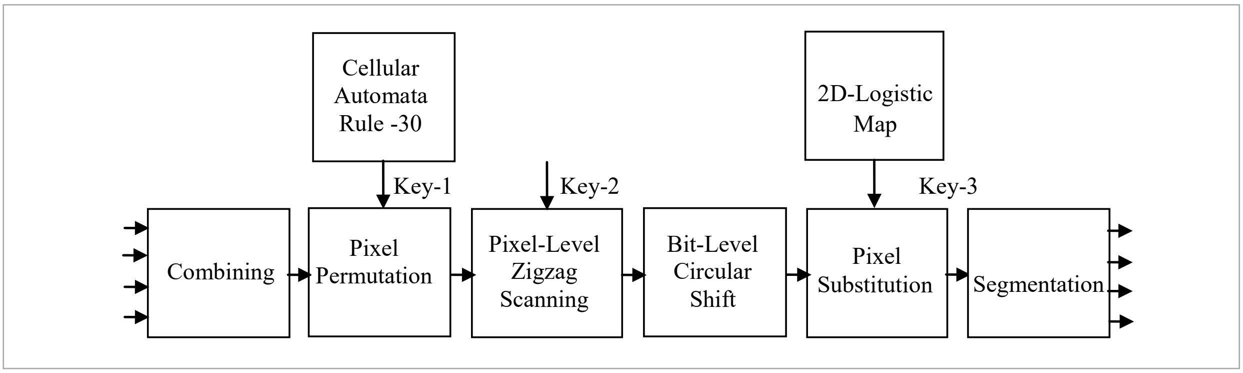
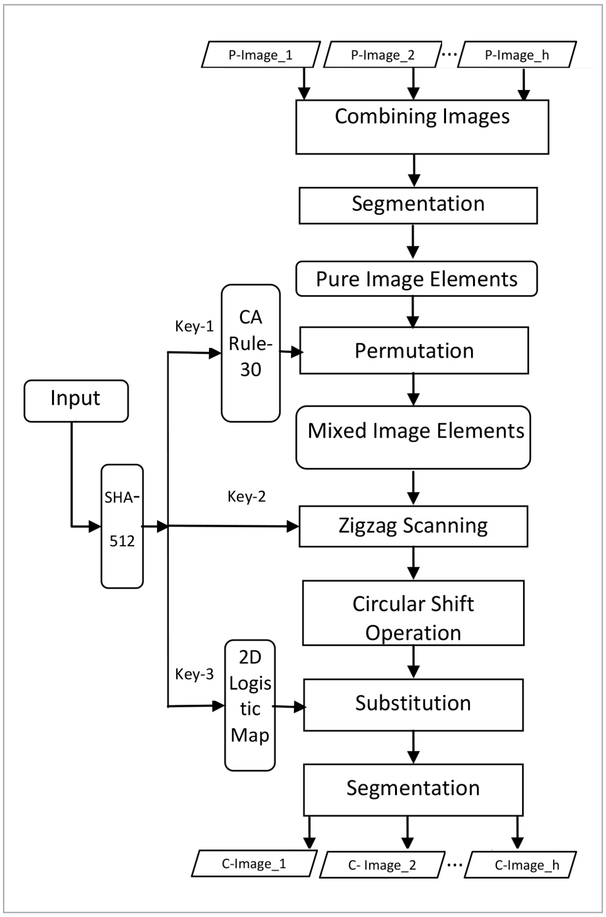


Figure 8

Flowchart of encryption process



mutation operation is employed on the pure-image elements to create mixed-image elements. In this work, a two-stage permutation operation is performed. The first stage of the permutation operation, based on Rule-30 of the elementary cellular automata, is as follows. The permutation is performed on both rows and columns. The two different initial configuration vectors $\{R_0^P$ and $C_0^P\}$ of the circular boundary ECA are obtained as presented in the key generation phase.

In accordance with Rule-30, the initial configuration vectors R_0^P and C_0^P ay self-evolve and can acquire two evolved configurations, $R_i^P = \{R_0^P,\ R_1^P\ , ..R_e^P\ ...\ ,\ R_m^P\}$ and $C_i^P = \{C_0^P,\ C_1^P\ , ..C_e^P\ ...\ ,C_n^P\}$, where e is the eth round configuration, and m and n denote the dimensions of the big-image matrix,(I).The R^P sequence is used for row permutation and the C^P sequence for column permutation. Figure 9 gives an example.

Row Permutation (RP):

Case 1: If $R_e^P(i)==R_{e-1}^P(i)$, every value of the ith row of the image matrix I_{e-1} is left, circularly shifted s_1 times.

Case 2: If $R_e^P(i)== 0$ and $R_{e-1}^P(i) == 1$, every value of the ith row of the image matrix I_{e-1} is left, circularly shifted s_2 times.

Case 3: If $R_e^P(i)== 1$ and $R_{e-1}^P(i) == 0$, every value of the ith row of the image matrix I_{e-1} is right, circularly shifted s_3 times.

s_1, s_2 and s_3 are calculated using Equation (5):

$$\begin{cases} s_1 = \mathrm{mod}(i \times 250, m) \\ s_2 = \mathrm{mod}(i \times 250, m) + 2\ . \\ s_3 = \mathrm{mod}(i \times 250, m) + 2 \end{cases} \tag{5}$$

Column Permutation (RP):

Case 1: If $C_e^P(j)==C_{e-1}^P(j)$, every value of the jth column of the image matrix I_{e-1} is upward, circularly shifted s_4 times.

Case 2: If $C_e^P(j)== 0$ and $C_{e-1}^P(j) == 1$, every value of the jth column of the image matrix I_{e-1} is upward, circularly shifted s_5 times.

Case 3: If $C_e^P(j)== 1$ and $C_{e-1}^P(j) == 0$, every value of the jth column of the image matrix I_{e-1} is downward, circularly shifted s_3 times.

s_4, s_5 and s_6 are calculated using Equation (6):

$$\begin{cases} s_4 = \mathrm{mod}(j \times 250, n) \\ s_5 = \mathrm{mod}(j \times 250, n) + 2. \\ s_6 = \mathrm{mod}(j \times 250, n) + 2 \end{cases} \tag{6}$$

Step 4: Transform the big image matrix into a one- dimensional vector with zigzag scanning.

Step 5: Perform the k-bit left circular shift operation on each pixel value.

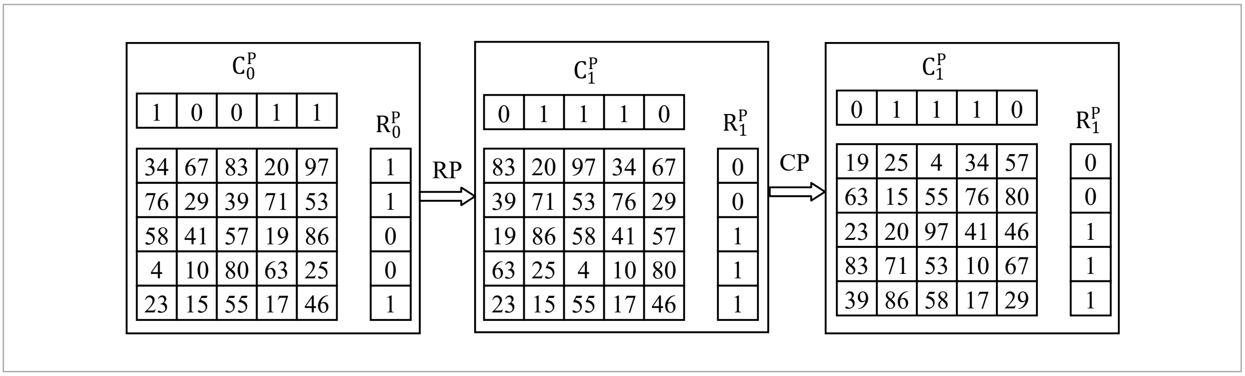
Step 6: Do the bitwise exclusive-or operation.

A pixel-level substitution based on the logistic map is performed in the proposed method, in which a new value is set for each pixel, as follows. The 2D logistic map (1) is iterated to obtain random sequences that are preprocessed in Equation (7) before being used. The simple exclusive-or operation is used in the pixel substitution process, as defined in Equation (8),

$$\begin{cases} X^s = x_i \times 10^{14} \bmod 256 \\ Y^s = y_i \times 10^{14} \bmod 256\ . \\ \quad Z^s = X^s \oplus Y^s \end{cases} \tag{7}$$

Figure 9

Permutation process based on CA



1	0	0	1	1	
34	67	83	20	97	1
76	29	39	71	53	1
58	41	57	19	86	0
4	10	80	63	25	0
23	15	55	17	46	1

0	1	1	1	0	
83	20	97	34	67	0
39	71	53	76	29	0
19	86	58	41	57	1
63	25	4	10	80	1
23	15	55	17	46	1

0	1	1	1	0	
19	25	4	34	57	0
63	15	55	76	80	0
23	20	97	41	46	1
83	71	53	10	67	1
39	86	58	17	29	1

Where I = 1, 2, ..., L (L is sequence length)

$$\begin{cases} R^c = \text{de2bi}\,(R_i) \oplus \text{de2bi}\,(x_i) \\ G^c = \text{de2bi}\,(G_i) \oplus \text{de2bi}\,(y_i)\,. \\ B^c = \text{de2bi}\,(B_i) \oplus \text{de2bi}\,(z_i) \end{cases} \quad (8)$$

Where (R, G& B) are color components.

Step 7: Segment the big image into h encrypted images.

3.3. Decryption Algorithm

Multiple-image decryption is the inverse of multiple-image encryption. The h enciphered images are combined into a big image, after which inverse pixel substitution is performed using the 2D logistic map, followed by the k-bit right circular shift operation on each pixel to restore the original pixel values. The pixel location is restored by carrying out inverse zigzag scanning and inverse pixel permutation using CA Rule-30. Finally, the big image is segmented to produce the h plain images

4. Experimental Setup

In all our experiments, we have used the MATLAB R2014a, Windows 7 software platform, the Intel Corei5-2.50GHz processor hardware platform and sixteen well-known RGB color images with pixels sized 128×128 were used. The parameters and initial seeds used for the logistic map were p_1=2.98, p_2 =3.30, q_1=0.18, q_2=0.15, x_s =0.898 and y_s =0.954. The test results are presented next, and compared with two peer image ciphers in the subsequent section. The 16 input images, combined big image and mixed-image elements are shown in Figures 10-12.

Figure 10

Input images

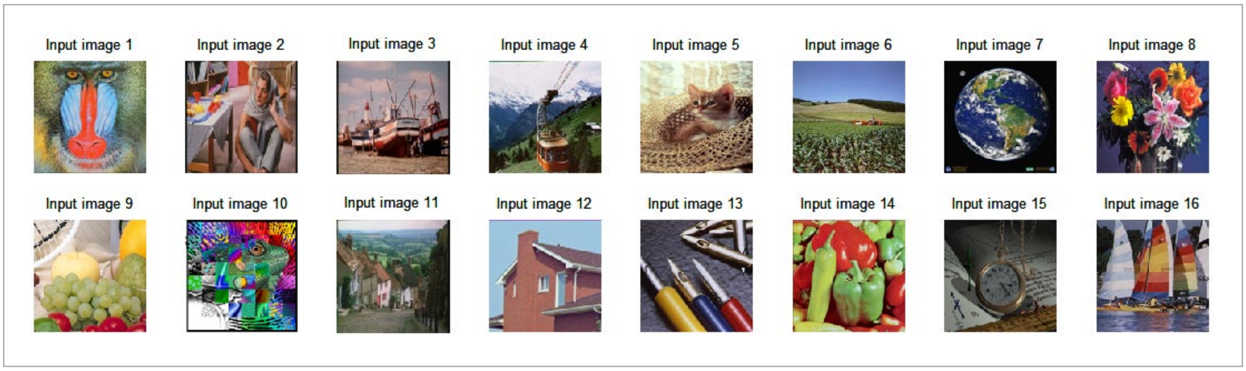


Figure 11

Big image

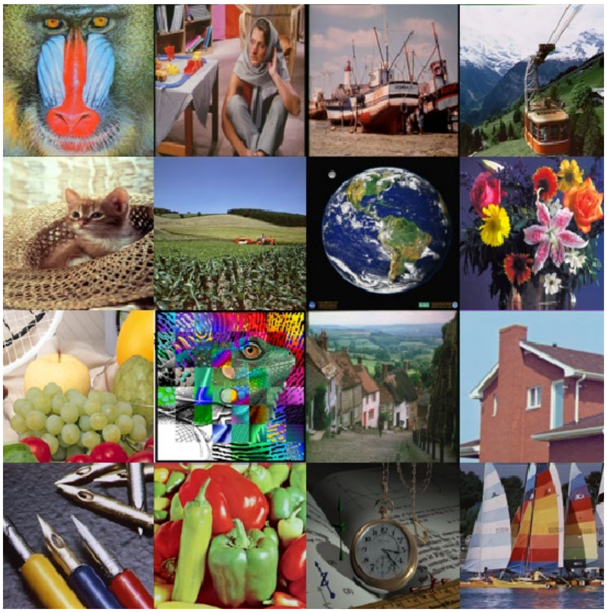
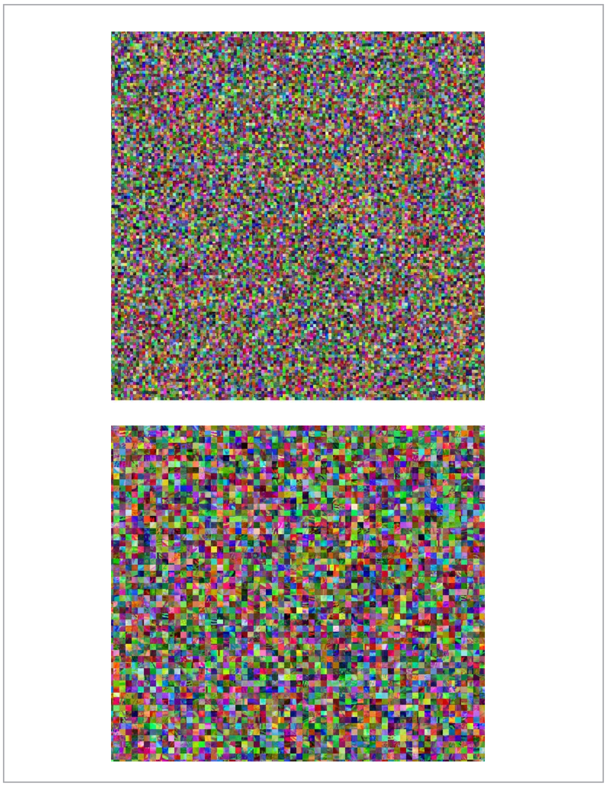


Figure 12

Mixed-image elements (with equal size 4×4 and 8×8)



5. Results Analysis

5.1. Input Sensitivity Test

The input image sensitivity test is used to assess the effectiveness of the cipher against chosen plain-image and known plain-image attacks [14]. In these attacks, the attackers compare two encrypted images to learn the relationship patterns between plain and cipher images. Such attacks are also referred to as differential attacks. The two well-known quantitative metrics, NPCR and UACI that are utilized to calculate the sensitivity of the cipher are defined in Equations (9 & 10) [35],

$$d(a,b) = \begin{cases} 0 & C^1(a,b) = C^2(a,b) \\ 1 & C^1(a,b) \neq C^2(a,b) \end{cases}, \quad NPCR = \frac{\sum_{a=1}^{w}\sum_{b=1}^{h} d(a,b)}{w \times h} \times 100\%, \tag{9}$$

$$UACI = \frac{\sum_{a=1}^{w}\sum_{b=1}^{h} \mid C^1(a,b)=C^2(a,b) \mid}{w \times h \times 255} \times 100\%, \tag{10}$$

where $C^1$and C^2 are the encrypted images of the plain images, P^1 and P^2 with P^1 and P^2 differing in exactly one pixel The obtained NPCR and UACI values are displayed in Table 1.

5.2. Key Space Analysis

The security strength of a cipher chiefly relies on the keys, which demand a large key space [3]. In this system, the starting position for zigzag scanning, starting values (real numbers) for the 2D logistic map and 512-bit hash constitute the secret key. Since the precision is set to 10^{14} in our experiment, the key space is approximately 2^{622}. Hence our proposed approach offers larger key space than schemes reported in [29, 30]. A bigger space repels all key-based attacks.

5.3. Key Sensitivity Analysis

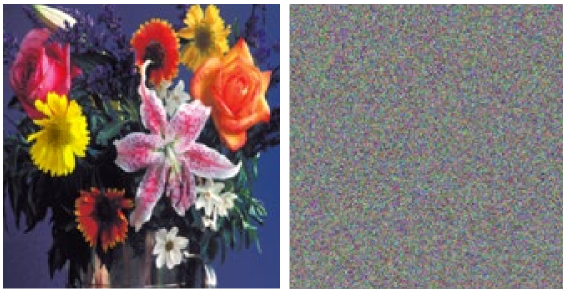
Sensitivity to keys is an excellent property of a good cipher, causing the encryption and decryption processes to produce entirely different output images when minor changes are made in the keys [33]. In our experiment, the key sensitivity is tested as follows. The input image is encrypted with the starting seeds [x_s=0.898 and y_s =0.954], following which a tiny change is made in one of the seeds [x_s=0.8980000000001], though other secret key values are not changed and decrypted with

Table 1
Experimental results of the NPCR and UACI

Input Image	NPCR				UACI			
	Proposed	[39]	[13]	[7]	Proposed	[39]	[13]	[7]
Input Image 1	99.5930	99.4653	99.4093	91.3786	33.4635	33.2438	33.3718	28.9313
Input Image 2	99.6520	99.5378	99.4951	88.9764	33.5599	33.4193	33.4253	27.4865
Input Image 3	99.5971	99.4256	99.4829	90.1651	33.5888	33.4917	33.3266	28.4621
Input Image 4	99.5910	99.5274	99.5012	90.4290	33.5063	33.4070	33.4637	28.1839
Input Image 5	99.6765	99.5630	99.4686	89.0002	33.4399	33.4057	33.5524	29.5397
Input Image 6	99.6195	99.5471	99.5442	88.0516	33.3662	33.4135	33.2379	28.1774
Input Image 7	99.5992	99.4524	99.5027	89.7114	33.4887	33.3604	33.4586	28.9430
Input Image 8	99.6236	99.5747	99.4849	91.4761	33.5228	33.2941	33.3480	29.1066
Input Image 9	99.5890	99.5634	99.6032	90.5400	33.3906	33.5576	33.3731	29.3281
Input Image 10	99.6154	99.5625	99.5073	88.2531	33.3877	33.5214	33.3552	29.0412
Input Image 11	99.6358	99.5951	99.6012	91.2153	33.2611	33.1845	33.2546	29.6280
Input Image 12	99.5768	99.5734	99.5632	89.5966	33.3290	33.3174	33.3948	28.3620
Input Image 13	99.5666	99.4869	99.4992	88.0473	33.5070	33.3934	33.4547	29.7208
Input Image 14	99.5829	99.5317	99.5175	88.1362	33.4093	33.4316	33.4058	29.4524
Input Image 15	99.6256	99.5436	99.5358	89.1763	33.3974	33.3623	33.3466	27.5867
Input Image 16	99.4583	99.4951	99.5114	88.3649	33.4521	33.3279	33.3733	29.0943

the unmodified and modified keys. The results displayed in Figure 13 show that the decrypted image with the slightly modified key is absolutely unintelligible, with no relation to the original images.

Figure 13
Key sensitivity analysis



(a)
Decrypted image-8 with the starting seeds (x_s=0.898 and y_s =0.954)

(b)
Decrypted image-8 with the starting seeds (x_s=0.8980000000001 and y_s=0.954)

5.4. Histogram Analysis

A histogram specifies the frequency occurrences of color values in an image [6]. Typically, since the histograms of plain images are different, the attacker exploits this statistical feature to compromise the cipher. To prevent such a threat, the statistical features of plain images must be destroyed by the cipher during encryption. The histograms of the 16 plain, encrypted and decrypted images are shown in Figure 14. The visual comparison makes it clear that while the cipher image histograms are almost similar and flat, the corresponding plain image histograms are intensified at a few value levels and, further, the decrypted image histograms are very similar to the original images. So then, it is concluded that the attacker cannot deduce valuable information through statistical attacks.

Figure 14

Histogram analysis

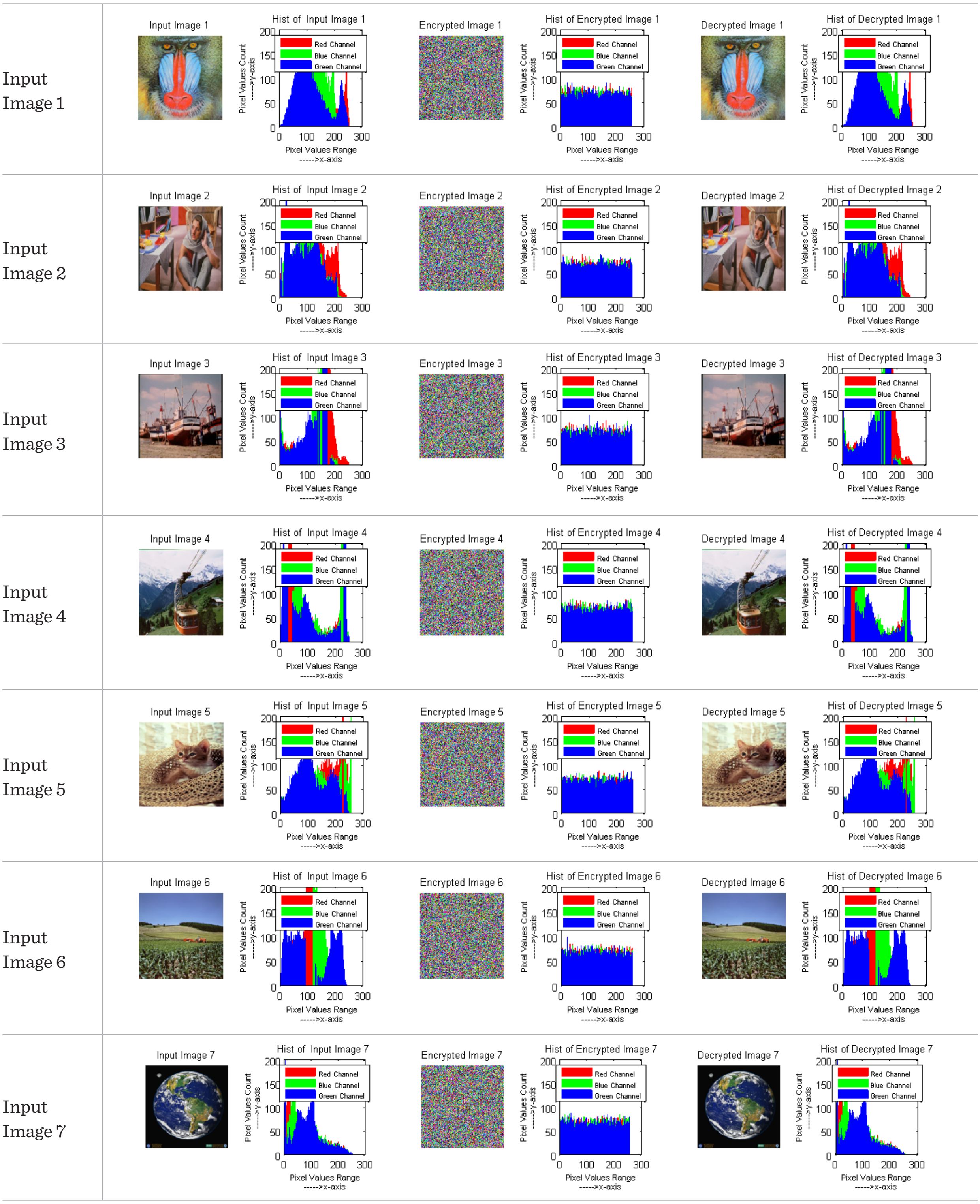


Figure 14 (continued)

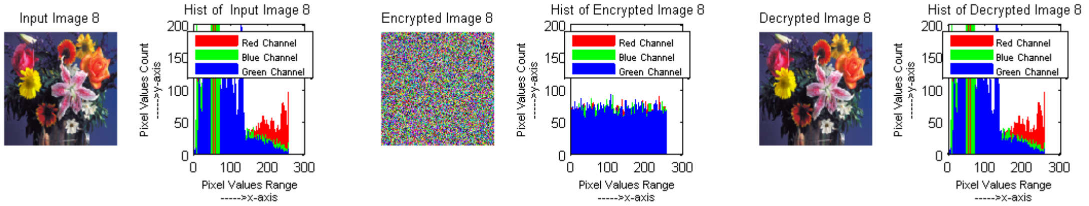
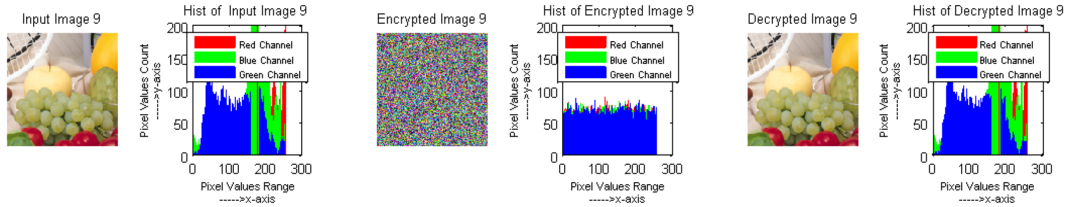
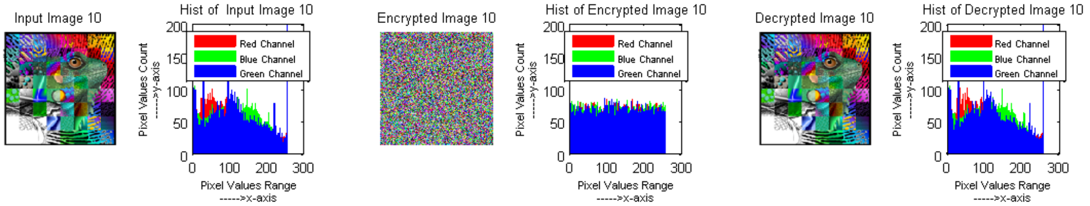
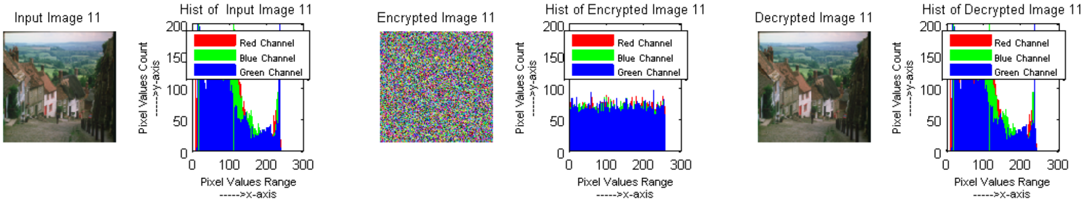
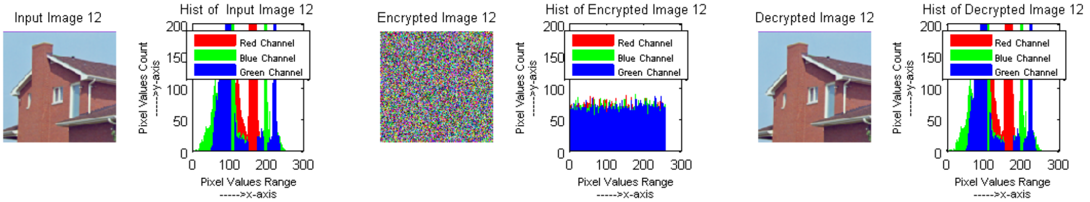
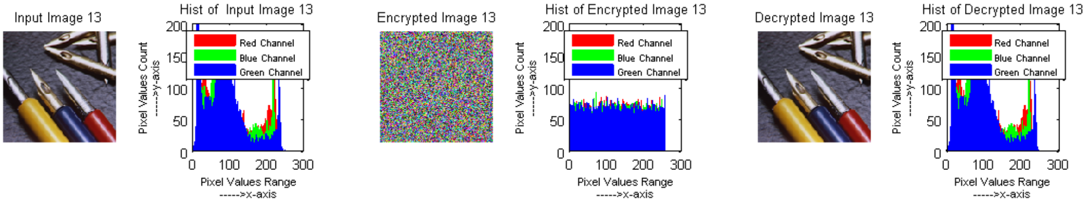
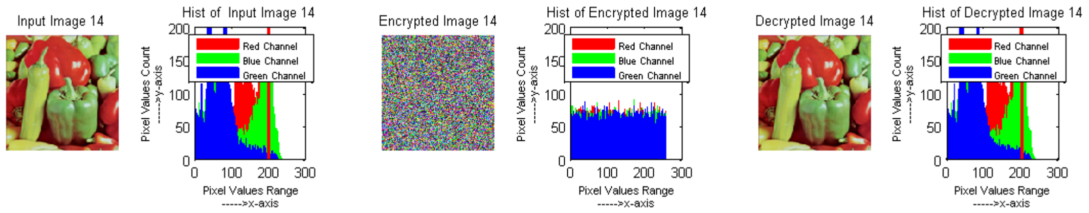
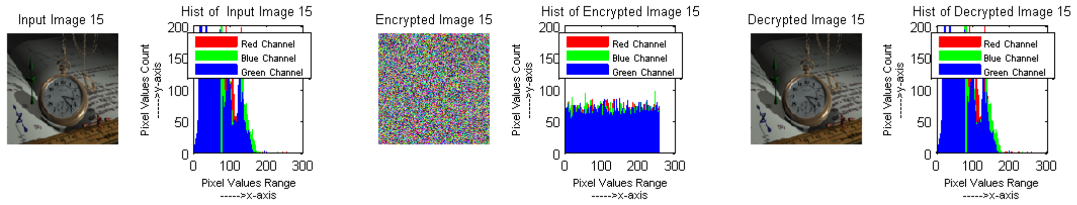
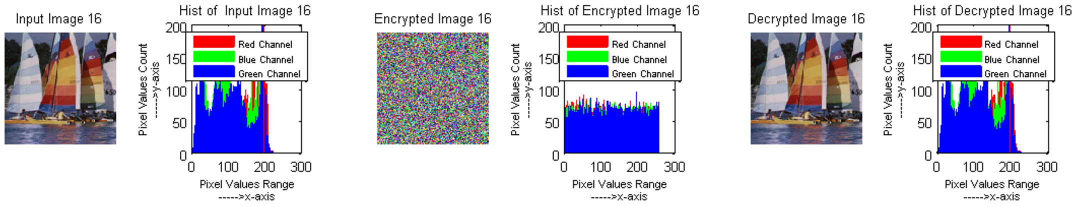
Input Image 8	
Input Image 9	
Input Image 10	
Input Image 11	
Input Image 12	
Input Image 13	

Figure 14 (continued)

Input Image 14	
Input Image 15	
Input Image 16	

5.5. Correlation Analysis

Correlation analysis measures the similarity association between neighbor pixel values [16]. Given that all natural plain images have a strong correlation, it is required that the encryption method assures a weak correlation in the encrypted images. To calculate the correlation in our work, 3000 pixel pairs were selected randomly in diagonal, vertical and horizontal directions, and the correlation measured using Equation (11):

$$\text{Corr\_Coff} = \frac{\text{cov(a,b)}}{\sigma_a \times \sigma_b}\,. \tag{11}$$

The correlation test results are listed in Table 2 (where V is vertical, H is horizontal and D is diagonal), and the correlation of input image1 and the corresponding encrypted image1is plotted in Figure 15. It is observed from the outcomes that the regular relevance between neighbor pixels is destroyed in the cipher image.

The encrypted image histograms are uniformely distributed (equal probability). Therefore, the proposed system withstands statistical attacks well.

5.6. Information Entropy (IE)

The metric, entropy, quantifies the randomness in the pixel value distribution of digital images. The standard entropy value for a true random image is 8 [3]. IE is calculated using Equation (12),

$$E(s) = \sum_{a=0}^{255} p(s_a) log_2\, p(s_a), \tag{12}$$

where $p(s_a)$ represents the emergence probability corresponding to s_a. Table 3 shows the entropy test results which indicate that this method has produced random images.

Table 2
Experimental result of correlation coefficient

Input Image	Direction	Plain Image	Proposed	[39]	[13]	[7]
			Encrypted			
Input Image 1	V	0.9252	0.0094	0.0318	0.0112	0.1067
	H	0.9120	-0.0163	0.0321	0.0251	0.1035
	D	0.8732	0.0077	0.0119	0.0148	0.1264
Input Image 2	V	0.9447	0.0015	0.0117	0.0427	0.1359
	H	0.8893	0.0072	0.0124	0.0830	0.1205
	D	0.8395	0.0049	0.0419	0.0375	0.0910
Input Image 3	V	0.9323	0.0053	0.0169	0.0174	0.1413
	H	0.9186	0.0065	0.0596	0.0494	0.1087
	D	0.8665	0.0009	0.0321	0.0526	0.1216
Input Image 4	V	0.9569	-0.0102	0.0147	0.0520	0.1407
	H	0.9696	0.0013	0.0314	0.0507	0.0926
	D	0.9391	0.0047	0.0238	0.0378	0.1047
Input Image 5	V	0.8982	0.0085	0.0137	0.0308	0.1187
	H	0.9409	0.0062	0.0157	0.0426	0.1202
	D	0.8669	0.0033	0.0154	0.0371	0.1372
Input Image 6	V	0.8504	-0.0126	0.0104	0.0350	0.1420
	H	0.8845	0.0061	0.0128	0.0208	0.0934
	D	0.8102	-0.0151	0.0174	0.0187	0.1380
Input Image 7	V	0.8977	0.0039	0.0283	0.0264	0.1504
	H	0.9300	-0.0049	0.0413	0.0252	0.1209
	D	0.8626	-0.0117	0.0396	0.0436	0.1388
Input Image 8	V	0.9355	-0.0145	0.0340	0.0285	0.1103
	H	0.8898	-0.0578	0.0157	0.0307	0.1346
	D	0.8599	0.0066	0.0189	0.0259	0.0137
Input Image 9	V	0.9588	0.0001	0.0478	0.0452	0.1088
	H	0.9526	-0.0102	0.0185	0.0446	0.1419
	D	0.9301	-0.0045	0.0141	0.0251	0.1060
Input Image 10	V	0.8224	0.0024	0.0346	0.0429	0.1535
	H	0.7952	0.0079	0.0238	0.0281	0.1017
	D	0.6776	-0.0119	0.0385	0.0307	0.1183
Input Image 11	V	0.9605	-0.0100	0.0117	0.0178	0.1609
	H	0.9456	-0.0070	0.0264	0.0253	0.1392
	D	0.9201	0.0057	0.0376	0.0196	0.1095
Input Image 12	V	0.9518	0.0060	0.0221	0.0281	0.1241
	H	0.9524	-0.0109	0.0279	0.0355	0.1077
	D	0.9178	-0.0098	0.0342	0.0393	0.0911
Input Image 13	V	0.9088	0.0015	0.0255	0.0306	0.1102
	H	0.9304	0.0008	0.0139	0.0349	0.1149
	D	0.9074	-0.0012	0.0236	0.0267	0.1026
Input Image 14	V	0.9580	-0.0041	0.0133	0.0254	0.1490
	H	0.9375	0.0019	0.0277	0.0326	0.1270
	D	0.9131	0.0057	0.0260	0.0229	0.1087
Input Image 15	V	0.9059	-0.0048	0.0310	0.0367	0.1069
	H	0.9123	0.0080	0.0348	0.0292	0.1074
	D	0.8759	0.0002	0.0294	0.0309	0.1036
Input Image 16	V	0.9243	-0.0153	0.0227	0.0367	0.1197
	H	0.8981	-0.0139	0.0384	0.0241	0.1384
	D	0.8292	0.0038	0.0281	0.0238	0.1139

Figure 15

Correlation coefficient of test image 8 before and after encryption

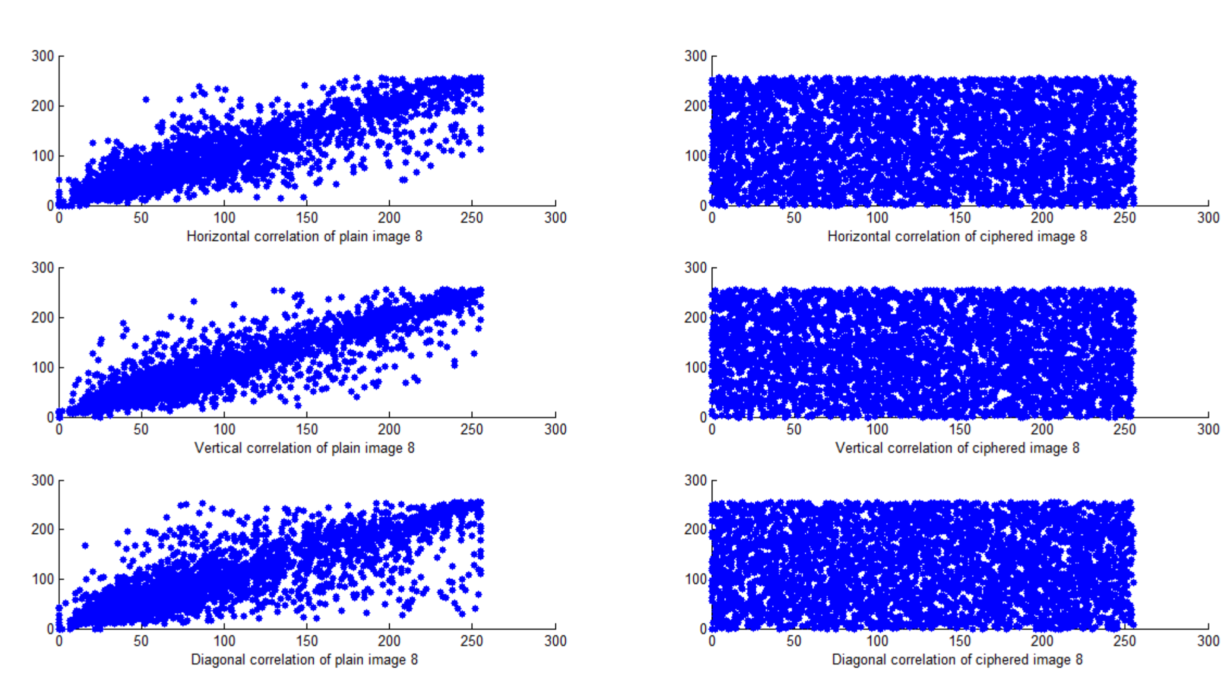


Table 3

Experimental results of information entropy and PSNR

Input Image	Information Entropy				PSNR			
	Proposed	[39]	[13]	[7]	Proposed	[39]	[13]	[7]
Input Image 1	7.9951	7.9859	7.9129	7.1963	90.7593	87.7240	85.1858	78.4542
Input Image 2	7.9957	7.9572	7.9348	7.1302	89.0605	85.1802	86.0631	75.2094
Input Image 3	7.9953	7.9429	7.9166	7.2618	90.0980	85.7106	83.9650	73.0816
Input Image 4	7.9966	7.9803	7.9217	7.1861	91.0714	86.5430	84.3320	74.4392
Input Image 5	7.9964	7.9481	7.9311	7.3730	88.7784	87.8093	85.2373	78.1687
Input Image 6	7.9965	7.9130	7.9367	7.1958	90.1624	86.1415	85.1917	75.8356
Input Image 7	7.9963	7.9802	7.9184	7.1535	89.6496	85.2286	84.8029	73.6731
Input Image 8	7.9959	7.9390	7.9497	7.1244	91.5455	85.1171	86.0731	73.4009
Input Image 9	7.9966	7.9197	7.9321	7.1800	87.8315	84.3052	84.8531	73.1182
Input Image 10	7.9963	7.9445	7.9469	7.1437	90.0058	86.1235	85.1805	76.0615
Input Image 11	7.9956	7.9523	7.9395	7.2273	87.2155	86.1595	86.2319	79.4071
Input Image 12	7.9957	7.9266	7.9172	7.2946	88.1991	85.6475	84.7642	74.2998
Input Image 13	7.9964	7.9902	7.9580	7.1184	90.8237	84.9348	84.8271	72.3307
Input Image 14	7.9964	7.9897	7.9259	7.1417	88.2931	85.6066	84.7689	78.0649
Input Image 15	7.9960	7.9631	7.9433	7.2092	88.1732	85.1279	85.4011	76.0311
Input Image 16	7.9959	7.9518	7.9347	7.1591	89.3171	86.0527	85.1865	77.8562

5.7. PSNR Analysis

The PSNR is an image quality index which judges the quality of deciphered images. Mathematically, it is calculated using Equation (13) [14],

$$PSNR = 10log_{10}(\frac{255}{MSE}), \tag{13}$$

wherein MSE represents the mean square error. The obtained PSNR test outcome is displayed in Table 3. From the results, it is concluded that the quality of images produced by the decryption process is good.

Time complexity analysis

The encryption time is analyzed to estimate the computation cost. To reduce the time consumption, we have used faster exclusive-or, integer addition and modulus operation in our proposed scheme. The encryption time is presented in Table 4. As can be seen in Table 4**,** the non-time consuming operations effectively accelerate the encryption process. The encryption speed is faster than references [13, 15, 39]**.** Therefore, this scheme can be used in real-time internet applications

Table 4
Computational time (unit: seconds)

Algorithms	Time
Proposed Algorithm	1.01630
Karawia et al. [13]	1.72811
Li et al. [15]	1.46385
Xiaoqiang et al. [39]	2.19654
Priya [7]	1.80739

NIST Statistical Test Analysis

NIST statistical test is a very important tool to assess the various aspects of randomness in a bit sequence [9]. The diversity of randomness in encrypted images was tested using NIST suite SP 800-22. This suite has 15 statistical tests. The randomness of a bit sequence is determined by p-value. The significant-level α = 0.02 is set to obtain p-value from 15 tests. Table 5 shows the statistical results of an encrypted image. The results proved that the proposed scheme has passed all the fifteen tests. Hence, the generated sequence is truly random.

Table 5
NIST statistical test results for encrypted image

NIST Test	p-value	D-R level	Result	Conclusion
Frequency	0.709101	2%	pass	random
Frequency (within a block)	0.581426	2%	Pass	random
Runs	0.800546	2%	pass	random
Longest run (once in a block)	0.354581	2%	pass	random
Rank (Binary matrix)	0.621956	2%	pass	random
FFT	0.378670	2%	pass	random
Non-overlapping template	0.425068	2%	pass	random
Overlapping template	0.259219	2%	pass	random
Universal	0.394625	2%	pass	random
Linear complexity	0.432408	2%	pass	random
Serial	0.565922	2%	pass	random
Approximate entropy	0.208502	2%	pass	random
Cumulative sums	0.501924	2%	pass	random
Random excursions	0.643127	2%	pass	random
Random excursions variant	0.301085	2%	pass	random

6. Discussion

The performance test results produced by the proposed technique is analyzed and compared here with three peer image ciphers based on performance metrics like the correlation coefficient, NPCR, PSNR, UACI and information entropy. Figure 12 depicts flat cipher image histograms, which means that the pixel values appear with equal probability. The total secret key space in this technique is approximately 2^{622}, which is remarkably high, and helps resist key-based attacks like brute force attacks. It is obvious from Figure 11 that the input image-based keys used in the proposed technique are so highly sensitive that even a small change in the keys produces a totally new decrypted image. From the numerical results listed in Table 2 and Figure 13, it is observed that the double permutation nature of the proposed technique excellently minimizes the correlation association among neighbor pixels, when compared to the other two techniques. The plain image sensitivity tests conducted, with the results presented in Table 1, show that the UACI and NPCR values obtained using the proposed method are optimal and counter differential attacks better than the other two methods. The PSNR image quality metric test results displayed in Table 3 show that the decrypted image quality is good, compared to that offered by the two peer schemes. The double substitution process yields the best entropy values for all the encrypted images. Overall, it is concluded that the proposed technique performs well in all tests.

7. Conclusion

A symmetric multiple color image encryption technique has been proposed that includes cellular automata, zigzag scanning, circular shifts, chaos and mixed-image content. This algorithm achieves two-stage encryption by adopting a dual permutation and dual substitution structure. The experimental outcomes and a comparison of the findings show that the dual permutation operation significantly minimizes the correlation association between neighbor pixels. The dual substitution helps produce the true random cipher image, thereby strengthening security. The combination of cellular automata and chaos increases the key space of the system. Moreover, the input image-based key generation method offers key sensitivity much-needed strong security. Finally, it is concluded that the proposed technique can be used in several areas to secure multiple color images simultaneously.

References

1. Alfalou, A., Brosseau, C., Abdallah, N., Jridi, M. Simultaneous Fusion Compression and Encryption of Multiple Images. Optics Express, 2011, 19, 24023-24029. https://doi.org/10.1364/OE.19.024023
2. Asadollahi, H., Kamarposhti, M. S., Jandaghi, E. M. Image Encryption Using Cellular Automata and Arnold Cat's Map. Australian Journal of Basic and Applied Science, 2011, 5, 587-593.
3. Banik, A., Shamsi, Z., Laiphrakpam, D. S. An Encryption Scheme for Securing Multiple Medical Images. Journal of Information Security and Applications, 2019, 49. https://doi.org/10.1016/j.jisa.2019.102398
4. Butusov, D. N., Pesterev, D. O., Tutueva, A. V., Kaplun, D. I., Nepomucenod, E. G. New Technique to Quantify Chaotic Dynamics Based on Differences Between Semi-Implicit Integration Schemes. Communications in Nonlinear Science and Numerical Simulation, 2021, 92. https://doi.org/10.1016/j.cnsns.2020.105467
5. Chai, X., Fu, X., Gan, Z., Zhang, Y., Lu, Y., Chen, Y. An Efficient Chaos-Based Image Compression and Encryption Scheme Using Block Compressive Sensing and Elementary Cellular Automata. Neural Computing and Applications, 2020, 32, 4961-4988. https://doi.org/10.1007/s00521-018-3913-3
6. Chen, X., Liu, Q., Wang, J., Wang, Q. Asymmetric Encryption of Multi-Image Based on Compressed Sensing and Feature Fusion with High Quality Image Reconstruction. Optics & Laser Technology, 2018, 107, 302-312. https://doi.org/10.1016/j.optlastec.2018.06.016
7. Deshmukh, P. An Image Encryption and Decryption Using AES Algorithm. International Journal of Scientific & Engineering Research, 2016, 7(2), 210-213.
8. Guo, L., Chen, J., Li, J. Chaos-Based Color Image Encryption and Compression Scheme Using DNA Complementary Rule and Chinese Remainder Theorem. International Computer Conference on Wavelet Active

Media Technology and Information Processing, 2016. https://doi.org/10.1109/ICCWAMTIP.2016.8079839

9. Hanis, S., Amutha, R. Double Image Compression and Encryption Scheme Using Logistic Mapped Convolution and Cellular Automata. Multimedia Tools Applications, 2018, 77, 6897-6912. https://doi.org/10.1007/s11042-017-4606-0

10. Harikrishnan, K. P., Nandakumaran, V. M. Bifurcation Structure and Lyapunov Exponents of a Modulated Logistic Map. Pramana-J. Phys, 1987, 29(6), 533-542. https://doi.org/10.1007/BF02845834

11. Jeyaram, B., Radha, R., Raghavan, R. New Cellular Automata-Based Image Cryptosystem and a Novel Non-Parametric Pixel Randomness Test. Security and Communication Network, 2016, 9, 3365-3377. https://doi.org/10.1002/sec.1542

12. Jin, J. An Image Encryption Based on Elementary Cellular Automata. Optics and Lasers in Engineering, 2012, 50, 1836-1843. https://doi.org/10.1016/j.optlaseng.2012.06.002

13. Karawia, A. A. Encryption Algorithm of Multiple-Image Using Mixed Image Elements and Two Dimensional Chaotic Economic Map. Entropy, 2018, 20. https://doi.org/10.3390/e20100801

14. Li, H., Wang, Y., Yan, H., Li, L., Li, Q., Zhao, X. Double-Image Encryption by Using Chaos-Based Local Pixel Scrambling Technique and Gyrator Transform. Optics and Lasers in Engineering, 2013, 51, 1327-1331. https://doi.org/10.1016/j.optlaseng.2013.05.011

15. Li, J., Liu, H. Colour Image Encryption Based on Advanced Encryption Standard Algorithm with Two-Dimensional Chaotic Map. IET Information Security, 2013, 7(4), 265-270. https://doi.org/10.1049/iet-ifs.2012.0304

16. Liu, H., Kadir, A., Sun, X., Li, Y. Chaos Based Adaptive Double-Image Encryption Scheme Using Hash Function and S-Boxes. Multimedia Tools Applications, 2018, 77, 1391-1407. https://doi.org/10.1007/s11042-016-4288-z

17. Liu, X., Mei, W., Du, H. Simultaneous Image Compression Fusion and Encryption Algorithm Based on Compressive Sensing and Chaos. Optics Communications, 2016, 366, 22-32. https://doi.org/10.1016/j.optcom.2015.12.024

18. Matthews, R. On the Derivation of a Chaotic Encryption Algorithm. Cryptologia, 1989, 13, 29-42. https://doi.org/10.1080/0161-118991863745

19. Mondal, B., Singh, S., Kumar, P. A Secure Image Encryption Scheme Based on Cellular Automata and Chaotic Skew Tent Map. Journal of Information Security and Applications, 2019, 45, 117-130. https://doi.org/10.1016/j.jisa.2019.01.010

20. Patro, K. A. K., Soni, A., Netam, P. K., Acharya, B. Multiple Grayscale Image Encryption Using Cross-Coupled Chaotic Maps. Journal of Information Security and Applications, 2020, 52. https://doi.org/10.1016/j.jisa.2020.102470

21. Perales, J. C. M. Color Image Encryption by Cellular Automata. Contemporary Engineering Sciences, 2015, 8, 1693-1701.https://doi.org/10.12988/ces.2015.510285

22. Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., Blažauskas, T. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic-Tent Map. Entropy, 2019, 21(7). https://doi.org/10.3390/e21070656

23. Sano, M., Sawada, Y. Measurement of the Lyapunov Spectrum from a Chaotic Time Series. Physical Review Letters, 1985, 55. https://doi.org/10.1103/PhysRevLett.55.1082

24. Sawlikar, A. P. An Efficient Double Image Compression and Encryption Technique. International Journal of Mechanical Engineering and Technology, 2018, 9(7), 1555-1563.

25. Sui, L., Lu, H., Wang, Z., Sun, Q. Double-Image Encryption Using Discrete Fractional Random Transform and Logistic Maps. Optics and Lasers in Engineering, 2014, 56, 1-12. https://doi.org/10.1016/j.optlaseng.2013.12.001

26. Sui, L., Duan, K., Liang, J. Double-Image Encryption Based On Discrete Multiple-Parameter Fractional Angular Transform And Two-Coupled Logistic Maps. Optics Communications, 2015, 343, 140-149. https://doi.org/10.1016/j.optcom.2015.01.021

27. Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A. M., Hirota, K., Abd EL-Latif, A. A. Design and Implementation of A Simple Dynamical 4-D Chaotic Circuit with Applications in Image Encryption. Information Sciences, 2020, 515, 191-217. https://doi.org/10.1016/j.ins.2019.10.070

28. Tsuchiya, T., Yamagishi, D. The Complete Bifurcation Diagram for the Logistic Map. Zeitschrift für Naturforschung, 1997, 52, 513-516. https://doi.org/10.1515/zna-1997-6-708

29. Tutueva, A. V., Nepomuceno, E. G., Karimov, A. I., Andreev, V. S., Butusov, D. N. Adaptive Chaotic Maps and

Their Application to Pseudo-Random Numbers Generation. Chaos, Solitons & Fractals, 2020, 133. https://doi.org/10.1016/j.chaos.2020.109615

30. Tutueva, A. V., Karimov, A. I., Moysis, L., Volos, C., Butusov, D. N. Construction of One-Way Hash Functions with Increased Key Space Using Adaptive Chaotic Maps. Chaos, Solitons & Fractals, 2020, 141. https://doi.org/10.1016/j.chaos.2020.110344

31. Wang, X., Luo, C. Bifurcation and Fractal of The Coupled Logistic Map. International Journal of Modern Physics, 2008, 22(24), 4275-4290. https://doi.org/10.1142/S0217979208038971

32. Wang, X., Zhang, Y., Zhao, Y. A Novel Image Encryption Scheme Based on 2-D Logistic Map and DNA Sequence Operations. Nonlinear Dynamics, 2015, 82, 1269-1280. https://doi.org/10.1007/s11071-015-2234-7

33. Wang, X., Gu, S., Zhang, Y. Novel Image Encryption Algorithm Based on Cycle Shift and Chaotic System. Optics and Lasers in Engineering, 2015, 68, 126-134. https://doi.org/10.1016/j.optlaseng.2014.12.025

34. Wolfram, S. Computation Theory of Cellular Automata. Communications in Mathematical Physics, 1984, 96), 15-57. https://doi.org/10.1007/BF01217347

35. Wu, Y., Noonan, J., Agaian, S. NPCR and UACI Randomness Tests for Image Encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2011.

36. Xiong, Y., Quan, C., Tay, C. J. Multiple Image Encryption Scheme Based on Pixel Exchange Operation and Vector Decomposition. Optics and Lasers in Engineering, 2018, 101, 113-121. https://doi.org/10.1016/j.optlaseng.2017.10.010

37. Zhang, L., Zhou, Y., Huo, D., Li, J., Zhou, X. Multiple-Image Encryption Based on Double Random Phase Encoding and Compressive Sensing by Using A Measurement Array Preprocessed with Orthogonal-Basis Matrices. Optics & Laser Technology, 2018, 105, 162-170. https://doi.org/10.1016/j.optlastec.2018.03.004

38. Zhang, X., Wang, X. Multiple-Image Encryption Algorithm Based on Mixed Image Element and Chaos. Computers & Electrical Engineering, 2017, 62, 401-413. https://doi.org/10.1016/j.compeleceng.2016.12.025

39. Zhang, X., Wang, X. Multiple-Image Encryption Algorithm Based On Mixed Image Element and Permutation. Optics and Lasers in Engineering, 2017, 92, 6-16. https://doi.org/10.1016/j.optlaseng.2016.12.005

40. Zhang, X., Wang, X. Multiple-Image Encryption Algorithm Based on the 3D Permutation Model and Chaotic System. Symmetry, 2018, 10.https://doi.org/10.3390/sym10110660

41. Zhang, X., Wang, W., Zhong, S., Yao, Q. Image Encryption Scheme Based on Balanced Two-Dimensional Cellular Automata. Mathematical Problems in Engineering, 2013. https://doi.org/10.1155/2013/562768

42. Zhong, Z., Chang, J., Shan, M., Hao, B. Double Image Encryption Using Double Pixel Scrambling and Random Phase Encoding, Optics Communications, 2012, 285, 584-588. https://doi.org/10.1016/j.optcom.2011.11.025

43. Zhou, N., Yang, J., Tan, C., Pan, S., Zhou, Z. Double-Image Encryption Scheme Combining DWT-Based Compressive Sensing with Discrete Fractional Random Transform. Optics Communications, 2015, 354, 112-121. https://doi.org/10.1016/j.optcom.2015.05.043

44. Zhou, N., Jiang, H., Gong, L., Xie, X. Double-Image Compression and Encryption Algorithm Based on Co-Sparse Representation and Random Pixel Exchanging. Optics and Lasers in Engineering, 2018, 110, 72-79. https://doi.org/10.1016/j.optlaseng.2018.05.014

45. Zhou, S., Wang, B., Zheng, X., Zhou, C. An Image Encryption Scheme Based on DNA Computing and Cellular Automata. Discrete Dynamics in Nature and Society, 2016. https://doi.org/10.1155/2016/5408529

46. Zhu, L., Song, H., Zhang, X., Yan, M., Zhang, L., Yan, T. A Novel Image Encryption Scheme Based on Nonuniform Sampling in Block Compressive Sensing. IEEE Access, 2019, 7, 22161-22174.https://doi.org/10.1109/ACCESS.2019.2897721