A Selective Self-adaptive Image Cryptosystem Based on Bit-planes Decomposition

Hossam Diab
(Corresponding author: Hossam Diab)

Computer Science Department, College of Computer Science and Engineering, Taibah University, KSA
Department of Mathematics and Computer Science, Faculty of Science, Menoufia University
Gamal Abd El-Nasir, Qism Shebeen El-Kom, Shebeen El-Kom, Menofia Governorate, Egypt
(Email: dr.hosamdiab@gmail.com, hdiab@taibahu.edu.sa)

(Received Feb. 13, 2018; revised and accepted June 18, 2018)

Abstract

The intrinsic traits of digital images, such as huge data, data redundancy, and tight relation of neighbor pixels, are usually difficult to handle by classical encryption techniques. Accordingly, this paper suggests an efficient self-adaptive image cryptosystem based on chaotic systems to satisfy the requirements of secure image storage and communication. The suggested cipher first decomposes the input plainimage into eight bit-planes and then divides the bit-planes into two groups. A chaotic based mechanism randomly selects two bit-planes to form the first group and the remaining bit-planes are assigned to the second group. The first group is then chaotically encrypted based on the information extracted from the second one along with two extra-generated bits. Further, the presented cipher independently masks the second group by a randomly created key stream related to the cipher pixel. Visually and computationally, the proposed cipher is extensively tested against different security attacks and the results confirm its good performance.

Keywords: Bit-Planes Decomposition; Chaos System; Image Encryption; Security Analysis; Self-Adaptive Encryption

1 Introduction

Digital images are considered one of the most significant information representation styles. Due to its features of visibility and abundance in information expression (most information we obtained is from vision perceiving), digital images are extensively used. Further, several intrinsic features like huge data size, high redundancy, and tight relation among pixels characterize digital images. Accordingly, most of the traditional cryptosystems (i. e. DES, AES, RC5, RC6, RSA, etc.) are not appropriate for practical image protection, indeed, most of these techniques are basically devoted to text data. Moreover, many of these techniques have been found insecure, particularly with respect to known and/or chosen-plaintext attacks. Consequently, special techniques to preserve valuable image information from illicit access should be developed. At present, many image cryptosystems have been presented to handle these issues. In particular, chaos-based ciphers are considered promising alternatives to the classical encryption techniques. Especially, the chaotic systems have several good properties such as pseudorandom property, sensitive dependence on initial system parameters, and non-periodicity which meet the basic requirements for secure cryptography. Generally, two primitive operations are widely employed for image encryption: pixel shuffling and pixel substitution. The shuffling process changes only the location of the pixel to remove the strong correlation between image pixels. On the other hand, the substitution process alters the values of the pixels to spread any slight change across the whole image. Accordingly, the image encryption techniques are classified into permutation-only ciphers, substitution-only ciphers or product ciphers that apply the two processes in consequence to achieve high level of security [17, 21, 22].

1.1 Literature Review

In this section, a brief overview of the techniques related to the present work is provided. Mitra *et al.* [21] presented a scheme that combines bit permutation, pixel permutation, and block permutation to protect digital images. The main features of this method are its simplicity and low computation load. However, a very large key size is required to accomplish bits, pixels, and blocks permutations, which accompanied with a flexibility problem for practical applications. Zhao *et al.* [47] studied the ergodic matrix ciphers (permutation-only ciphers) and developed an efficient decryption algorithm for cracking these ciphers. Further, Li *et al.* [15] demonstrated that all permutation-only based ciphers can be broken through known/chosen-plaintext attacks. In addition, Jolfaei and

Wu [9] developed an optimal chosen plainimage attack to crack the pure permutation ciphers. Accordingly, it is found that the secret permutation alone cannot afford adequate security levels for image security applications.

He *et al.* [7] introduced an encryption technique based on a new dynamic system that incorporates an S-box and an XOR plus mod operations. Their scheme relied on a new constructed nonlinear chaotic mapping to thwart the grey code and statistical attacks. However, Li [11] discovered a serious flaw of the encryption function in [7] and showed that the cipher method can be cracked with only two selected plainimages. Tong *et al.* [29] utilized a compound chaotic system to design a two-phase image cryptosystem. Specifically, Tong scheme incorporated two phases: in the first phase, the image pixels are substituted with XOR operation. While in the second phase, a circular shift position permutation is applied to the masked image. The two phases are governed by a pseudo-random sequence produced by compound system of two related chaotic maps. Li *et al.* [13] scrutinized the security aspects of Tong scheme [29] and pointed out that the cryptosystem can be broken with only three chosen plainimages. Furthermore, they demonstrated that the scheme is not adequately sensitive to the modifications of the plainimages. Pareek *et al.* [25] introduced an image cipher in which eight distinct kinds of operations are utilized to mask the image data. A main feature of Pareek scheme is the derivation of the initial conditions of the chaotic map via an external secret key. Li *et al.* [12] discussed the security issues of the encryption method presented in [25]. They found several problems in Pareek scheme such as invalid keys, a number of equivalent keys and weak keys, which shrink the key space of the cryptosystem. Also, they developed some attacks to a number of sub keys. In addition, they proposed a known plainimage attack model to break the scheme. Wang *et al.* [33] introduced an encryption method in which the plaintext is encrypted using alternant of the stream and block ciphers. A pseudo-random sequence is employed to determine which cipher mode is selected. The Wang cryptosystem can be applied to several types of files such as JPEG, DOC, TXT, and WMA. Abdo *et al.* [1] presented an image cryptosystem in which a special type of periodic boundary elementary cellular automata is employed. In this algorithm, different key streams are generated depending on the chaotic cellular neural network to encrypt different plainimages. Xiao *et al.* [39] suggested an image cipher in which the Cat map is exploited to shuffle the image pixels and the Chen chaotic system is employed to disguise the values of image pixels. Lian *et al.* [18] presented an image cryptosystem that permutes the plainimage by the $2D$ standard map and further diffuses the shuffled image by the Logistic map. Wang and Teng [32] presented a novel image cryptosystem which uses a Logistic map to produce scrambling sequences, shuffle and diffuse the RGB channels. Tu *et al.* [30] analyzed the scheme presented in [32] and reported that the cryptosystem is vulnerable to chosen plaintext attack. Specifically, the analysis reveals that the permutation sequence and the diffusion key stream are fixed and independent from the plaintext which enables the opponent to launch the given attack. Parvin *et al.* [26] developed an image encryption scheme involving rows and columns scrambling followed by a substitution process. Their scheme utilized a combination of two $1D$ chaotic maps to generate three random sequences to complete the encryption mapping. Norouzi and Mirzakuchaki [23] analyzed the design issues of the cipher in [26] and employed a chosen plainimage attack to break the scheme by recovering an equivalent key stream used in the diffusion stage and consequently the two shuffling sequences of the permutation stage.

Additionally, based on the excellent properties of bit-level scrambling, which simultaneously modifies the pixel location and its value; several image cryptosystems employing bit permutation have been presented in the literature. Zhu *et al.* [49] presented an image cipher that exploits the chaotic Cat map for bit-level shuffling and diffuses the image pixels depending on the chaotic Logistic map. Xiang *et al.* [37] suggested a selective image cipher in which the most significant four bits of each pixel are only encrypted and the least significant four bits are left intact. Yen and Guo [42] introduced a bit-level cryptosystem in which the primitive operation of bit rotation is employed to mask the image pixels. Teng and Wang [28] presented an image cryptosystem based on chaotic systems and self-adaptive that carries out its operation at bit-level. Liu and Wang [19] developed a color image encryption scheme based on the piecewise linear chaotic map and Chen chaotic system. Specifically, the proposed approach permuted the plainimage at bit-level and simultaneously masked the color components using Chen system. Xu *et al.* [40] developed a novel chaotic cipher based on the primitive operations of cyclic shift; bit-Xor and swapping that are employed at bit-level of the image. Zhou *et al.* [48] used the bit-planes of an auxiliary image as a security key to chaotically encrypt the plainimage. Li *et al.* [16] developed an image cipher using a hyper-chaotic system by applying pixel-level and bit-level scrambling. Zhang *et al.* [43] combined a lightweight bit-level permutation and cascade cross circular diffusion to encrypt the plainimages to remedy the flaws related to the classical chaotic encryption architecture. Zhang *et al.* [44] investigated the key features of image bit-planes information and their distribution. Further, a novel confusion structure using a proposed expand-and-shrink approach was presented to encipher color images. Hoang and Thanh [8] identified the defects of the encryption scheme proposed in [44] and demonstrated that the cipher lacked the dependency on the plainimage information for the diffusion operation. Moreover, they reported other flaws arisen from the isolated location of affected values in the decryption. Finally, they restored an equivalent lookup table for permutation through a chosen cipherimage attack. Diaconu [4] proposed a novel image cipher that applies a new circular inter-intra pixels bit-level scrambling mechanism to enhance the encryption effect. Cao *et al.* [2] developed a novel chaotic map based on the combination of Logistic map and iterative chaotic map with infinite collapse ($ICMIC$) using a cascade modulation couple model. Additionally, they employed the new map in designing a novel image cipher by applying bit-level scrambling and diffusion simultaneously. Fu *et al.* [6] presented a new bit-level scrambling strategy using Cat map for designing a secure cipher for medical image applications. Zhang and Wang [46] developed a new image cipher by utilizing the spatiotemporal dynamics of non-adjacent coupled map lattices. They presented a novel bit-level shuffling mechanism that transmits the bits of one bit-plane to any other bit-plane. As a result, the statistical properties of the bit-planes are altered and the key features of the image are disguised. Ye [41] employed the Logistic map to produce a pseudo-random stream for scrambling the bits information of the plainimage. Fu *et al.* [5] introduced a two-phase bit-level scrambling process that results in a considerable diffusion effect by employing Chebyshev map and Cat map. Wang *et al.* [34] combined the chaotic coupled map lattice and DNA computing to design an efficient image cipher. The image pixels are firstly masked by a pseudo-random stream generated from the chaotic map and then encoded by employing the DNA operations. Finally, the cipher image is gained by applying the DNA-level permutation, DNA-level substitution, and DNA decoding in consequence. Wang and Luan [31] presented a novel image cryptosystem by merging the reversible cellular automata and the intertwining Logistic map to apply the permutation-substitution structure at bit level. Zhang *et al.* [45] suggested a novel image cryptosystem using $3D$ bit matrix shuffling. The scheme combined the Chen chaotic system and a $3D$ Cat map to define a new shuffling rule for plainimage permutation. Further, it confused the shuffled image by a chaotic key stream generated by employing the Logistic map. Wu *et al.* [36] analyzed the image cipher introduced in [45] and demonstrated its potential flaws of the employed $3D$ cat map and insensitivity to the changes of the plainimage. Further, they presented a chosen plainimage attack model that successfully cracked the underlying scheme. In addition, an improved variant of the scheme was proposed to overcome the identified shortcomings of the original scheme. Li *et al.* [14] presented a novel attack model based on chosen-plainimage attack to crack the permutation-diffusion ciphers. They divided this architecture into two independent models (permutation and diffusion) and then separately broke each model to firstly restore the diffusion key stream and secondly recover the permutation sequence. Moreover, to prove the feasibility of the proposed model, they successfully attacked the cipher presented in [45]. Liu *et al.* [20] proposed a cryptosystem that handles the plainimage at bit-level. Firstly, the image pixels are permuted by a random chaotic sequence generated from the improved Logistic map. Secondly, the permuted image is decomposed into eight bit-planes and the lower four bits are fed to the improved Logistic map to create a key stream related to the plainimage. Thirdly, the key stream is adjusted to shuffle and mask the higher four bits. Finally, the encrypted image is obtained by combining the masked higher four bits and the lower four bits into one pixel.

1.2 Contribution and Organization of the Paper

In this paper, an effective image cryptosystem based on chaotic systems is suggested to satisfy the needs of secure image transfer. The suggested scheme depends on a self-adaptive mechanism that employs the information extracted from a selected group of image bit-planes to make the encryption result related directly to the plainimage. The proposed cipher can efficiently mask the bit-planes information of the plainimage. Specifically, the proposed scheme is a fully parameterized mapping that is entirely dependent on the plainimage information. Namely, the parameters of the utilized chaotic systems are strongly correlated to the plainimage along with the secret key materials. Accordingly, for two trivially different images (only one bit differs), their associated key streams are completely distinct. Thus, the suggested cryptosystem can effectively fight all sorts of attacks including the most powerful chosen/known plainimage attack.

The rest of this paper is arranged as follows: Section 2 describes the basic tools required for constructing the proposed cipher. Section 3 depicts the details of the suggested cipher. Simulated results and security tests of the suggested cipher are introduced in Section 4 and Section 5, respectively. Finally, Section 6 draws the main conclusions of the paper.

2 Preliminaries

In this section, the basic theory related to bit-planes decomposition, Sine-Sine map and $3D$ intertwining Logistic map that are employed in our design is briefly discussed.

2.1 Bit-planes Decomposition

For the gray-images, the pixel value is represented in eight bits, so the brightness of the pixel is ranging from 0 to 255. Accordingly, each pixel of the image can be transformed into 8 bits representation as follows:

$$P(i,j) = Bp_8\ Bp_7\ Bp_6\ Bp_5\ Bp_4\ Bp_3\ Bp_2\ Bp_1 \quad (1)$$

where $P(i,j)$ is the pixel value at coordinate (i,j) and $Bp_k \in \{0,\ 1\}$ is the k^{th} bit of the pixel. Thus, eight different binary images can be obtained by collecting the k^{th} bit from each pixel. The k^{th} binary image represents the k^{th} bit-plane of the original gray-image. Figure 1 depicts the different 8 bit-planes for the Pirate plainimage. It is noticed that, based on the location of the bit in the image pixel, it weighted by 2^k to introduce a different amount of information for that pixel [28].

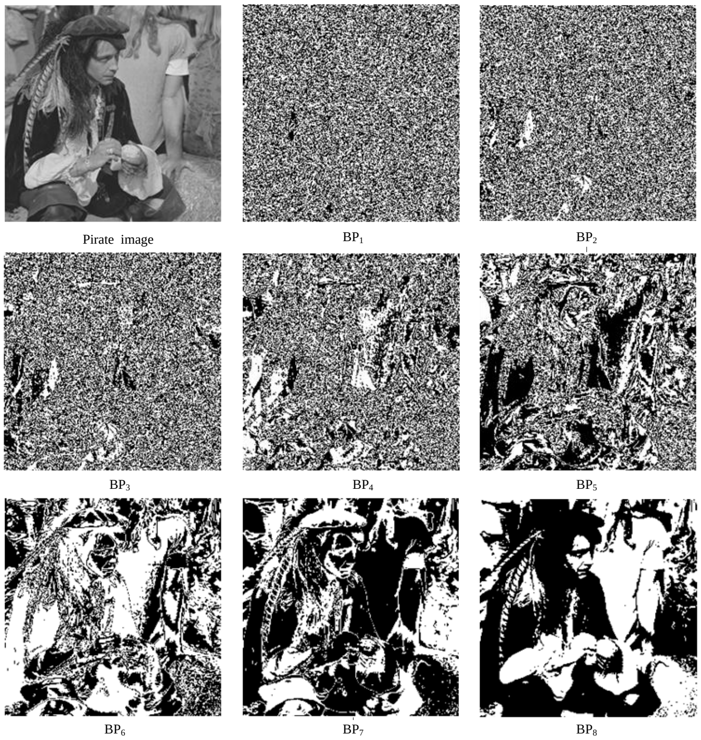

Figure 1: Bit-planes decomposition of Pirate plainimage

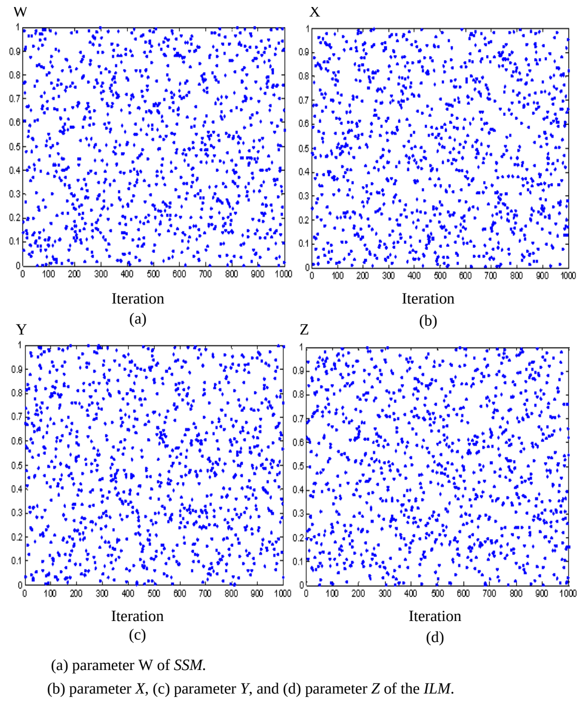

Figure 2: Chaotic behavior of the SSM and ILM

2.2 The Employed Chaotic Maps

Due to their simple structure and good chaotic properties, the classical chaotic maps such as Chebyshev map, Logistic map, Sine map, and Tent map, etc., have been commonly employed in designing image cryptosystems. However, several weaknesses related to such maps (for example, its limited chaotic range, blank windows, and uneven distribution of generated values, weak keys, etc.) degrade the performance of the encryption algorithm. Thus, to mitigate such flaws, Sine-Sine map (SSM) is designed in [24] and an intertwining Logistic map (ILM) is presented in [27].

The Sine-Sine map (SSM) is described by Equation (2):

$$W_i = u_1 \times \sin(\pi \times W_{i-1}) \times 2^{14} - floor(u_1 \times \sin(\pi \times W_{i-1}) \times 2^{14}), i = 1, 2, \ldots \quad (2)$$

where $u_1 \in (0, 10]$ and W_0 denote the control parameter and the initial value of the system, respectively. Figure 2a shows the outstanding chaotic behavior of the SSM which reveals the wide range of chaotic system without any of the aforementioned flaws.

Further, the $3D$ intertwining Logistic map (ILM) is defined by Equation (3):

$$\begin{aligned} X_i &= (u \times K_1 \times Y_{i-1} \times (1 - X_{i-1}) + Z_{i-1}) \bmod 1 \\ Y_i &= (u \times K_2 \times Y_{i-1} + \frac{Z_{i-1}}{(1 + X_i^2)}) \bmod 1 \\ Z_i &= (u \times (X_1 + Y_i + K_3) \times \sin(Z_{i-1})) \bmod 1 \end{aligned} \quad (3)$$

where the operation (r mod 1) returns the fractional part of the real number r by subtracting or adding an appropriate integer number, for example, (12.1234 mod 1) yields 0.1234 by subtracting the integer value 12, while (-12.1234 mod 1) returns 0.8766 by adding the integer value 13. Moreover, with the conditions of $0 < u \leq 3.999$, $|K_1| > 33.5$, $|K_2| > 37.9$, and $|K_3| > 35.7$, the map has brilliant chaotic features, and all weaknesses associated to simple maps are completely resolved. Additionally, the secret key is greatly expanded. Figure 2b, Figure 2c and Figure 2d depict the behavior of the intertwining map.

Pak and Huang [24] and Sam *et al.* [27] studied the chaotic performance of the SSM and the ILM, respectively, and demonstrated the good features of these maps. Both maps can solve the defects associated with the simple maps, which are mentioned above. Actually, the SSM and the ILM present several advantages to the proposed cipher including: 1) Their chaotic sequences are uniformly distributed within the interval $[0, 1]$ and effectively occupied the entire data range. 2) Both maps have a wide chaotic range, as demonstrated in [24, 27] by investigating the Lyapunov exponent of the maps. That is, the Lyapunov exponent of these maps is always positive in the entire range of the control parameters, which indicates the good chaotic behavior. Further, this wide range of the control parameters extends the key space of the cryptosystem. 3) the cascading of these maps together in our design reduces the dynamic degradation problems related to simple chaotic maps under the finite precision implementation and also enlarges the key space of the suggested scheme. Accordingly, these two chaotic sys-

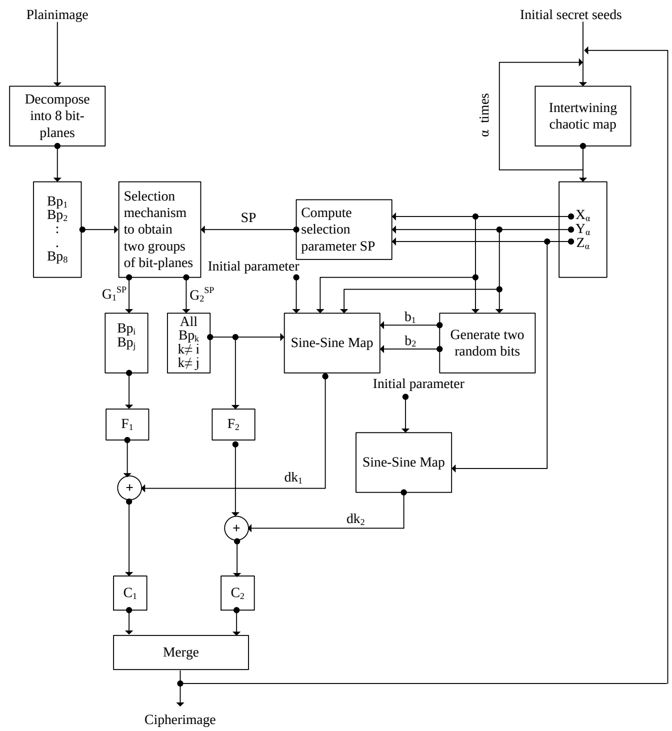

Figure 3: Architecture of the suggested cipher

tems will be exploited here for building an efficient image cryptosystem that uses the control parameters and initial values of both maps as a secret encryption key.

3 Suggested Image Cryptosystem

3.1 The Encryption Algorithm

This section depicts the framework of the suggested image cryptosystem in details. Firstly, the input plainimage is decomposed into 8 bit-planes. Afterward, two groups of bit-planes are chaotically selected at each pixel. One group is encrypted based on the information contained in the other group. Secondly, the second group is chaotically encrypted and then merged with the first group to obtain the ciphered pixel. Meanwhile, the parameters of the employed chaotic system are adapted at each encryption step based on the encrypted image information to yield different chaotic sequences for different plainimages. Figure 3 illustrates the proposed architecture of the suggested cipher. Specifically, the encryption process of the suggested cryptosystem can be depicted as follows:

Step 1: Decompose the input plainimage P into 8 bit-planes BP_1, BP_2, $\ldots$, and BP_8 as illustrated in Equation (1).

Therefore, in this step each bit-plane BP_i represents a binary image that contains a certain amount of plainimage information. This amount is proportional to the specific position (weights) of the bits in the original image pixels as depicted in Section 2.1.

Step 2: Iterate the intertwining Logistic map, given in Equation (3), α times using the initial values of its parameters u, K_1, K_2, K_3, X_0, Y_0, and Z_0.

This step generates three random values X_α, Y_α, and Z_α that carry the features of the chaotic map such as ergodicity, random like behavior, and high sensitivity to initial control parameters. Additionally, the initial values of the map parameters (u, K_1, K_2, K_3, X_0, Y_0, and Z_0) are used as a part of the secret key of the cipher. Accordingly, they contribute in extending the key-space of the suggested cipher to withstand the brute force attacks.

Step 3: Obtain temporary secret bits b_1 and b_2 according to Equation (4) and Equation (5), respectively.

$$b_1 = \begin{cases} 1 & \text{if } X_\alpha \geq 0.5 \\ 0 & otherwise \end{cases} \tag{4}$$

$$b_2 = \begin{cases} 1 & \text{if } Y_\alpha \geq 0.5 \\ 0 & otherwise \end{cases} \tag{5}$$

where X_α, and Y_α are the current states of ILM system.

Equation (4) and Equation (5) state that the two values b_1 and b_2 are chaotically generated based on the intertwining Logistic map outputs X_α and Y_α and they are highly correlated to the initial secret parameters of the map. Thus, slightly different initial parameters will produce different random bits for b_1 and b_2. Accordingly, the proposed cipher has a high sensitivity to tiny changes of secret key.

Step 4: Quantize the value of the obtained chaotic states X_α, Y_α, and Z_α to get the selection parameter SP according to Equation (6).

$$SP = ((X_\alpha + Y_\alpha + Z_\alpha) \times 10^{14}) \bmod 4 \tag{6}$$

Equation (6) demonstrates that the selection parameter SP is also related to the outputs of the intertwining Logistic map so it depends on the secret key of the cipher. In addition, it is clear that $SP \in \{0, 1, 2, 3\}$ to constitute four different combinations that determine the form of two bit groups G_1^{SP} and G_2^{SP} as described in Step 5.

Step 5: Split the set of image bit-planes into two groups G_1^{SP} that contains two bit-planes (BP_i and BP_j) and G_2^{SP} that includes the remaining bit-planes ($BP_k \ni k \neq i$ and $k \neq j$) according to Equation (7) and Equation (8), respectively.

$$G_1^{SP} = \begin{cases} [BP_1, BP_2] & \text{if } SP = 0 \\ [BP_3, BP_4] & \text{if } SP = 1 \\ [BP_5, BP_6] & \text{if } SP = 2 \\ [BP_7, BP_8] & \text{if } SP = 3 \end{cases} \tag{7}$$

$$G_2^{SP} = \begin{cases} [BP_3, BP_4, BP_5, BP_6, BP_7, BP_8] & \text{if } SP = 0 \\ [BP_1, BP_2, BP_5, BP_6, BP_7, BP_8] & \text{if } SP = 1 \\ [BP_1, BP_2, BP_3, BP_4, BP_7, BP_8] & \text{if } SP = 2 \\ [BP_1, BP_2, BP_3, BP_4, BP_5, BP_6] & \text{if } SP = 3 \end{cases} \quad (8)$$

Step 6: Iterate the Sin-Sin map, given in Equation (2), T times using the initial parameter W_0, computed according to Equation (9), and control parameter u_1 which is a part of the secret key.

$$W_0 = (\sum_{i=1}^{8} V_i \times 2^{-i} + X_\alpha + Y_\alpha) \bmod 1 \quad (9)$$

where V is the vector composed from concatenating the two generated bits (b_1 and b_2) and the bits of the second bit pattern G_2^{SP} obtained by Equation (8). Namely, V can be expressed as follows:

$$V = [b_1, b_2, G_2^{SP}] \quad (10)$$

where G_2^{SP} is defined in Equation (8).

Equation (9) computes the initial value of the Sin-Sin map based on the current output of the intertwining Logistic map in addition to the plainimage information contained in the second selected group G_2^{SP} along with the random bits b_1 and b_2. That is, the final generated value W_T of the Sin-Sin map is strongly related to the plainimage information and the secret key. Accordingly, this step makes the proposed cipher a self-adaptive algorithm that employs the information extracted from a selected group of image bits to encrypt the other group.

Step 7: Encrypt the first group G_1^{SP} according to Equation (11).

$$C_1 = F_1(G_1^{SP}) \oplus dk_1 \quad (11)$$

where $F_1(G_1^{SP})$ and the diffusion key dk_1 are computed according to Equation (12) and Equation (13), respectively.

$$F_1(G_1^{SP}) = \sum_{i=1}^{2} G_1^{SP}(i) \times 2^{i-1} \quad (12)$$

$$dk_1 = ((round(W_T \times 10^{14})) \bmod 257) \bmod 4 \quad (13)$$

Equation (11) masks the plainimage information of the group G_1^{SP} by the diffusion key dk_1 which is chaotically computed based on W_T as stated by Equation (13). Accordingly, the diffusion key is also related to the plainimage. That is, different plainimages will have different diffusion keys and hence, the proposed cipher can resist the chosen plaintext/ciphertext attacks.

Step 8: Compute a diffusion key dk_2 by iterating the Sin-Sin map, in Equation (2), N times using the initial parameter Z_α, obtained in Step 2, and the control parameter u_2, which is a part of the secret key according to Equation (14).

$$dk_2 = (round(W_N \times 10^{14})) \bmod 2^6 \quad (14)$$

Note that the modulus in Equation (14) equals 2^6 since the second group is composed of 6 bits that represents a value ranging from 0 to 63.

Step 9: Encrypt the second group G_2^{SP} according to Equation (15).

$$C_2 = F_2(G_2^{SP}) \oplus dk_2 \quad (15)$$

where $F_2(G_2^{SP})$ is computed according to Equation (16).

$$F_2(G_2^{SP}) = \sum_{i=1}^{6} G_2^{SP}(i) \times 2^{i-1} \quad (16)$$

Step 10: Obtain the cipher pixel by merging C_1 and C_2. The merge operation can be depicted as follows:

Step 10.1: Convert C_1 and C_2 into two-bit and six-bit values, respectively; and flip them to obtain C_1' and C_2' according to Equation (17) and Equation (18), respectively.

$$C_1' = Flip(dec2bin(C_1, 2)) \quad (17)$$

$$C_2' = Flip(dec2bin(C_2, 6)) \quad (18)$$

where $dec2bin(x, n)$ converts x into a binary value of length n and $Flip(x)$ is employed to read the input bit pattern in a reverse order from right to left.

Step 10.2: Concatenate C_1' and C_2' to obtain 8-bit length value and transform it to decimal value C.

$$C = bin2dec(C_1' || C_2') \quad (19)$$

Step 11: Update the initial parameters of the intertwining Logistic map to be used in the next encryption according to Equation (20).

$$\begin{aligned} X_0 &= (X_\alpha + \frac{C}{255}) \bmod 1 \\ Y_0 &= (Y_\alpha + \frac{C}{255}) \bmod 1 \\ Z_0 &= (Z_\alpha + \frac{C}{255}) \bmod 1 \end{aligned} \quad (20)$$

Equation (20) adjusts the parameters of the intertwining Logistic map based on the previous encrypted pixel to make all generated chaotic values, the random bits (b_1, b_2), and the diffusion keys ($dkey_1$ and $dkey_2$) for all subsequent pixels dependent on the plainimage information. Thus, this step also introduces a self-adaptive mechanism to the proposed cipher to ensure a high resistance against different types of attacks. In addition, this adaptation results in a different chaotic behavior of the employed chaotic maps.

Step 12: Repeat the steps from 2 to 11 to encrypt all image pixels.

On the other hand, for the decryption operation, the recipient can decrypt the cipherimage and correctly recover the plainimage by applying the same steps of the encryption process in a reverse order using the correct initial secret values. Also, all adjusted chaotic parameters related to the ciphered pixels can be computed during the decryption by the same method employed in the encryption procedure.

3.2 Design Considerations for the Proposed Cipher

The proposed method is a bit-level encryption that decomposes the plainimage into 8 bit-planes and then divides them into two groups of two bits and six bits, respectively. The motivations for this particular decomposition include: 1) to assign a different amount of plainimage information to each group. Indeed, this decomposition may assign variant weights to the bits of each group as depicted in Equation (12) and Equation (16). 2) Since the first group is encrypted based on the information of the second group, we put most of the plainimage bits on the second group to make the generated key stream more related to the plainimage data. 3) The most important point is that this particular decomposition can be simply extended to DNA representation. Particularly, DNA computing uses only 2-bit to encode the data in DNA representation. Indeed, the future work will focus on this extension to combine DNA computing and hyperchaotic systems for designing a new image cryptosystem. Moreover, the suggested architecture is simple and flexible so it can be adapted to work on two or more groups of bit-planes. Each group may contain any number of bits. For example, the algorithm can be slightly modified to handle two groups with an equal number of bits. The first group may contain the most significant 4 bits of the pixel and the second group includes the least significant 4 bits of the pixel.

The suggested cryptosystem employs multi chaotic systems cascading together to mitigate the dynamic degradation of a single chaotic system under the finite precision computation. Namely, the algorithm utilizes three chaotic maps including intertwining Logistic map and two Sin-Sin maps. The good chaotic behavior of these maps guarantees a better performance of the suggested cipher. Further, employing several chaotic maps extends the key-space of the algorithm. Specifically, nine parameters of the employed maps represent the secret key of the scheme, which make the key-space very large to resist exhaustive search attack.

Moreover, the scheme applies a self-adaptive encryption mechanism that exploits the features of the bit group G_2^{SP} to encrypt the first group G_1^{SP} to satisfy a dependency on the input plainimage. This dependency assures that the proposed cipher can withstand the chosen plainimage/cipherimage attacks. In addition, the parameters of the deployed chaotic maps are dynamically adjusted based on the encrypted information. That is, the chaotic behavior of the maps is affected by the input plainimage. Also, this adjustment of the parameters makes the generated random bits (b_1 and b_2) and the diffusion keys ($dkey_1$ and $dkey_2$) strongly related to the plainimage. Thus, different plainimages will have different encryption key streams and hence the scheme can counter any type of attacks. Finally, the merge operation presented in step 10 involves a permutation process (simple reverse operation of bits) to increase the confusion/diffusion features of the suggested cipher. Accordingly, the proposed cryptosystem can be effectively utilized for image encryption applications as demonstrated by the conducted experiments presented in Section 4 and Section 5.

4 Experimental Results

In this section, a variety of experimental tests are presented to demonstrate the efficiency of the suggested cryptosystem. In addition, to judge the encryption quality of the proposed cipher, we numerically compare its results with the schemes of Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20]. In our experimental results, several images are evaluated. These image, shown in Figure 4, are Lena, Airplane, Pirate, Lake, and TestPat. Specifically, to numerically evaluate the encryption quality of these cryptosystems, three estimation criteria are used. These criteria are the mean square error (MSE), peak signal to noise ratio ($PSNR$), and structural similarity index metric ($SSIM$) which can be computed by Equation (21), Equation (22), and Equation (23), respectively [27, 35, 38].

$$MSE = \frac{1}{M\times N}\sum_{r=1}^{M}\sum_{s=1}^{N}\Big(P(r,s)-C(r,s)\Big)^2 \tag{21}$$

where P, C, M, and N are the plainimage, its corresponding cipherimage, the height, and the width of the image, respectively.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{22}$$

$$SSIM = \frac{\left(2\mu_P\mu_C+\varepsilon_1\right)\left(2\sigma_{PC}+\varepsilon_2\right)}{\left(\mu_P^2+\mu_C^2+\varepsilon_1\right)\left(\sigma_P^2+\sigma_C^2+\varepsilon_2\right)} \tag{23}$$

where μ_P and μ_C are the mean for the images P and C, respectively. σ_P^2, σ_C^2, and σ_{PC} represent the variance of P, the variance of C, and the covariance between P and C, respectively. Finally, ε_1 and ε_2 denote two predefined quantities.

An interesting experiment that demonstrates the capability of the suggested cipher to hide plainimage patterns is displayed in Figure 4 in which the encryption and decryption results associated to the five plainimages are depicted. Obviously, the suggested method conceals

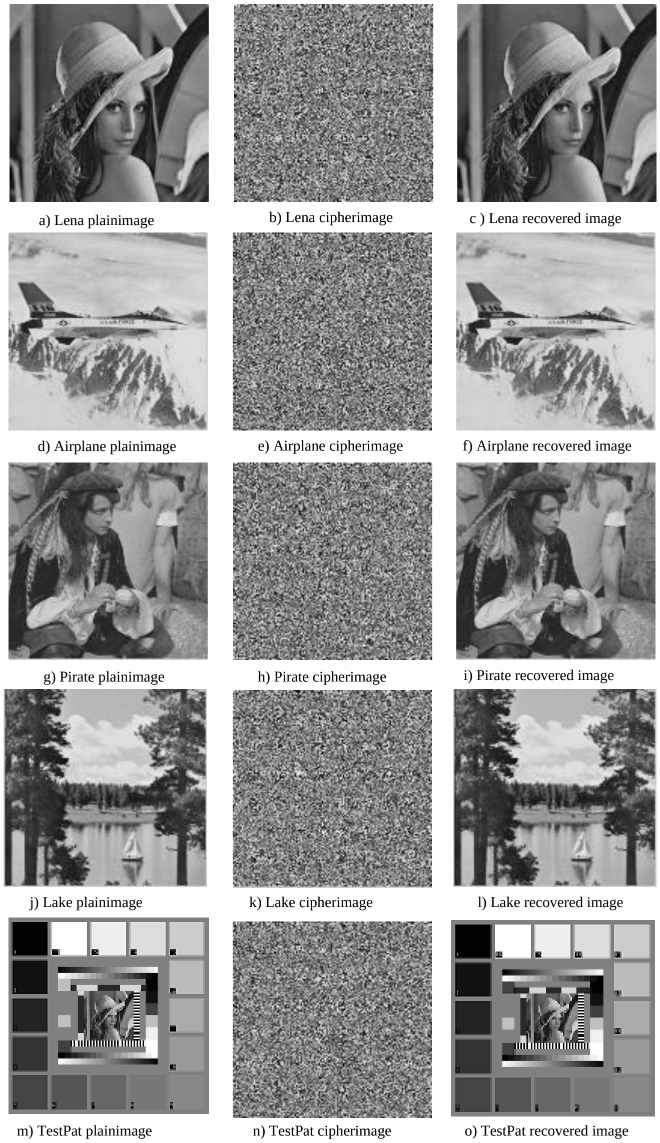

Figure 4: Encryption and decryption of the suggested image cryptosystem

all structures of the plainimages where the encrypted images are notably different from their corresponding original images, namely, the regular visual information of the plainimages can not be perceived in the ciphered images. Computationally, the obtained values of MSE, $PSNR$, and $SSIM$ related to the proposed cipher, Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20] are shown in Table 1, Table 2 and Table 3, respectively. The results reflect that there is a negligible relation between the plainimages and their corresponding ciphered images. Further, it is clear that the suggested cipher outperforms the schemes presented in [2,20,34,40,46] because it yields the largest average value for MSE and the smallest average value of $PSNR$, and $SSIM$.

Another example that confirms the feasibility of the suggested cryptosystem for color images is shown in Figure 5 and the related numerical values are depicted in Table 4. The results of this experiment demonstrate that the proposed cipher is also very effective in encrypting the color images.

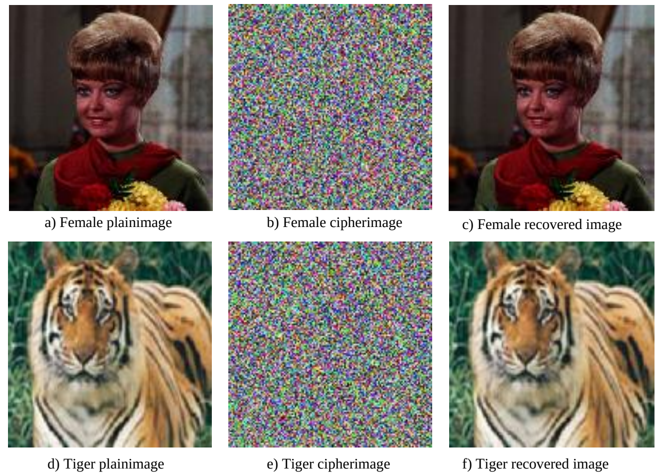

Figure 5: Feasibility of the suggested cryptosystem for color images

Table 1: Numerical evaluation based on MSE criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	8650.1	8697.3	8756	8691.5	8752.5	8767.7
Airplane	10120	10115	10123	10128	10130	10132
Pirate	7875.4	7844.1	7869.4	7880	7863.4	7889.3
Lake	9694.4	9672.7	9688.9	9632.4	9681.2	9699.6
TestPat	9753.3	9751.1	9693.9	9728.7	9747.4	9774.3
Average	9218.64	9216.04	9226.24	9212.12	9234.9	9252.58

Table 2: Numerical evaluation based on PSNR criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	8.7606	8.7369	8.7078	8.7399	8.7095	8.7019
Airplane	8.0790	8.0811	8.0778	8.0755	8.0747	8.0740
Pirate	9.1681	9.1853	9.1714	9.1655	9.1747	9.1604
Lake	8.2656	8.2753	8.2681	8.2934	8.2715	8.2633
TestPat	8.2393	8.2403	8.2658	8.2502	8.2419	8.2299
Average	8.5025	8.5038	8.4982	8.5049	8.4945	8.4859

Table 3: Numerical evaluation based on SSIM criterion

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	0.0113	0.0057	0.0050	0.0093	0.0056	0.0022
Airplane	0.0041	0.0077	0.0071	0.0098	0.0074	0.0108
Pirate	0.0064	0.0183	0.0072	0.0025	0.0075	0.0093
Lake	0.0085	0.0051	0.0056	0.0123	0.0064	0.0063
TestPat	0.0016	0.0063	0.0083	0.0083	0.0077	0.0028
Average	0.0064	0.0086	0.0066	0.0084	0.0069	0.0063

5 Security Analysis

A secure image cryptosystem must thwart all forms of attacks, including ciphertext-only attack, known plaintext

Table 4: Numerical evaluation of the proposed cipher for color images

Images	Femal			Tiger		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
Red	10075	8.0984	0.0004	10093	8.0906	0.0019
Green	12892	7.0277	0.0090	7969.9	9.1163	0.0061
Blue	13487	6.8315	0.0048	8691.1	8.7401	0.0006
Average	12151.33	7.3192	0.0047	8918	8.649	0.0029

attack, brute force attack, and statistical attack [17, 21, 22]. Herein, the security tests on the proposed scheme are thoroughly performed. These tests include the key space test, key sensitivity test, statistical test and plaintext sensitivity test(differential attack). Different tests attest that the suggested cipher provides a reasonable security level. In our experiments, the plainimages of Lena, Airplane, Pirate, Lake, and TestPat shown in Figure 4 have been investigated and the simulated results are displayed for illustration. Moreover, according to the structure of the suggested cipher which correlates the chaotic parameters with the plainimage/cipherimage, the cipher is strongly immune to ciphertext-only, chosen plaintext, and known plaintext attacks.

5.1 Key Space Analysis

An essential property for a secure image cipher is the high sensitivity to the cipher keys. Further, to defend against brute force attacks, the key space of the cipher must be sufficiently large [1, 24, 25]. The key space test on the proposed cryptosystem is carried out and the results are summarized here.

Key space: The suggested cipher, as previously stated, uses the control parameters and initial conditions of the intertwining Logistic map and Sine-Sine map as a secret key. So, the secret key includes the parameters ($u, K_1, K_2, K_3, X, Y, Z, u_1$, and u_2). Accordingly, the proposed cipher has $10^{135} > 2^{115}$ of different possible combinations of secret keys for a double-precision implementation. Thus, a cryptosystem with such large key space is reliable for image security applications and also can effectively defy the brute force attack.

Key sensitivity test: An attractive property of an ideal cryptosystem is its sensitivity to the secret key, namely, a minor modification in the secret key parameters (changing only one bit of the encryption key) must result in an entirely different ciphered image. To check the key sensitivity of the suggested cryptosystem, the subsequent steps are performed:

1) The secret key (key_1 that contains the set of initial values of chaotic maps used) is employed to encrypt the plainimage P and the resulted encrypted image is denoted as E_1;

2) The secret key (key_1) is slightly modified, by changing only one bit of one secret parameter, to get a closely related key (key_2) and the same plainimage P is encrypted again to get the ciphered image E_2;

3) Finally, the difference between the two enciphered images E_1 and E_2 is evaluated.

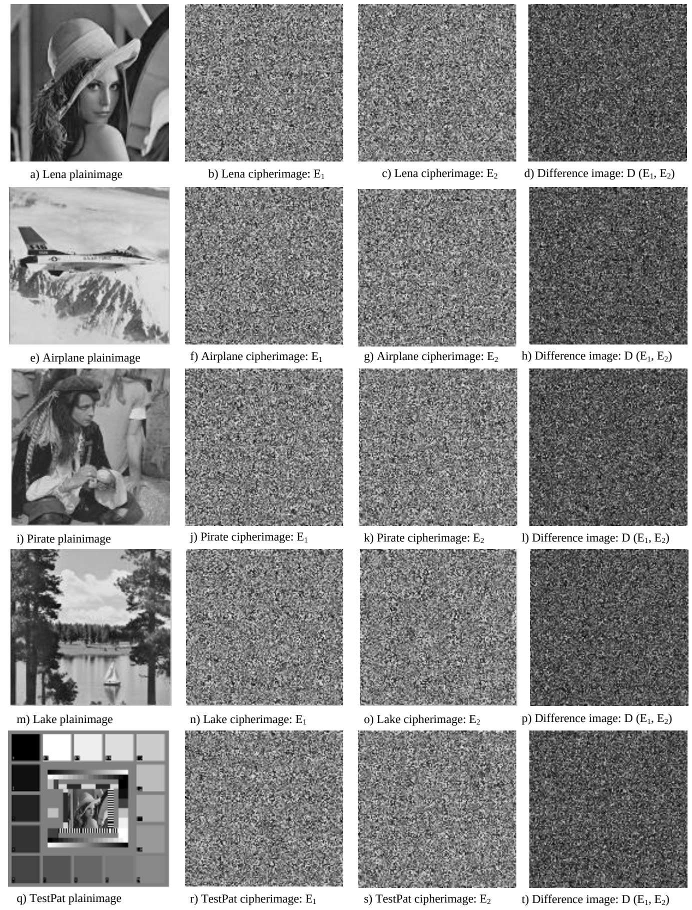

Figure 6: Results of key sensitivity for the suggested cryptosystem

Figure 6 illustrates the original plainimages, the two cipherimages obtained in the aforementioned steps, and the difference image $D(E_1, E_2)$, for each image, respectively. Notably, the difference images shown in Figure 6 confirm that the associated two cipherimages are totally distinct.

Furthermore, to computationally measure the difference between the two enciphered images E_1 and E_2, the correlation coefficient (CC), the number of pixels change rate ($NPCR$) and the unified average changing intensity ($UACI$) are computed. The CC, $NPCR$, and $UACI$ measures are depicted in Equation (24), Equation (25), and Equation (26), respectively [10, 44, 46].

$$CC = \frac{E(Z-E(Z))(w-E(w))}{\sqrt{D(z)}\sqrt{D(w)}} \quad (24)$$

where

$$D(z) = \frac{1}{N}\sum_{i=1}^{N}(z_i - E(z))^2 \text{ and } E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i$$

$$\text{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \qquad (25)$$

where

$$D(i,j) = \begin{cases} 0 & \text{if } E_1(i,j) = E_2(i,j) \\ 1 & otherwise \end{cases}$$

$$\text{UACI} = \frac{1}{M \times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(\frac{|E_1(i,j) - E_2(i,j)|}{255}\right)\right) \times 100\% \qquad (26)$$

The results of the key sensitivity test in terms of $NPCR$, $UACI$, and CC are displayed in Table 5, Table 6, and Table 7, respectively. The obtained values denote that there is a negligible correlation and a considerable difference among the enciphered images although they are generated by slightly different encryption keys. For instance, the enciphered image of Lena using key_1 has 99.62% (on average) of difference from the image enciphered using key_2 in terms of the pixel gray values, even though there is a single bit change between the two encryption keys. Note that, the first row of the tables specifies the modified parameter of key_1 to obtain key_2.

Table 5: Key sensitivity of the suggested method based on $NPCR$

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	99.60	99.64	99.66	99.61	99.62	99.60	99.62	99.63	99.62	99.62
Airplane	99.62	99.61	99.60	99.61	99.59	99.62	99.59	99.58	99.60	99.60
Pirate	99.62	99.59	99.62	99.61	99.63	99.63	99.63	99.64	99.60	99.62
Lake	99.59	99.60	99.63	99.63	99.59	99.60	99.60	99.61	99.63	99.61
TestPat	99.64	99.62	99.65	99.65	99.64	99.64	99.61	99.63	99.60	99.63
Average	99.61	99.61	99.63	99.62	99.61	99.62	99.61	99.62	99.61	

Table 6: Key sensitivity of the suggested method based on $UACI$

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	33.50	33.47	33.53	33.51	33.55	33.56	33.49	33.62	33.48	33.52
Airplane	33.49	33.49	33.47	33.46	33.53	33.45	33.49	33.53	33.50	33.49
Pirate	33.44	33.49	33.44	33.48	33.47	33.49	33.48	33.48	33.49	33.47
Lake	33.41	33.46	33.49	33.51	33.48	33.52	33.62	33.50	33.49	33.50
TestPat	33.47	33.51	33.54	33.49	33.60	33.52	33.60	33.50	33.51	33.53
Average	33.46	33.48	33.49	33.49	33.53	33.51	33.54	33.53	33.49	

Table 7: Key sensitivity of the suggested method based on CC

Image	X_1	X_2	X_3	K_1	K_2	K_3	U	U_1	U_2	**Average**
Lena	0.0024	0.0035	0.0029	0.0025	0.0089	0.0012	0.0013	0.0065	0.0004	0.0033
Airplane	0.0015	0.0003	0.0040	0.0004	0.0043	0.0015	0.0001	0.0036	0.0034	0.0021
Pirate	0.0026	0.0005	0.0016	0.0001	0.0025	0.0008	0.0020	0.0045	0.0053	0.0022
Lake	0.0051	0.0006	0.0030	0.0019	0.0016	0.0027	0.0090	0.0022	0.0012	0.0030
TestPat	0.0008	0.0016	0.0001	0.0010	0.0048	0.0015	0.0044	0.0023	0.0004	0.0019
Average	0.0025	0.0013	0.0023	0.0012	0.0044	0.0015	0.0034	0.0038	0.0021	

Furthermore, when the decryption key is slightly modified (trivially different from the encryption key), the recovering of the plainimage also absolutely fails. Figure 7 indicates that the image enciphered by key_1 (image E_1) is not properly recovered using key_2 (image RI), even though there is only a single bit change between the keys used for encryption and decryption. Thus, the suggested scheme is extremely sensitive to encryption key.

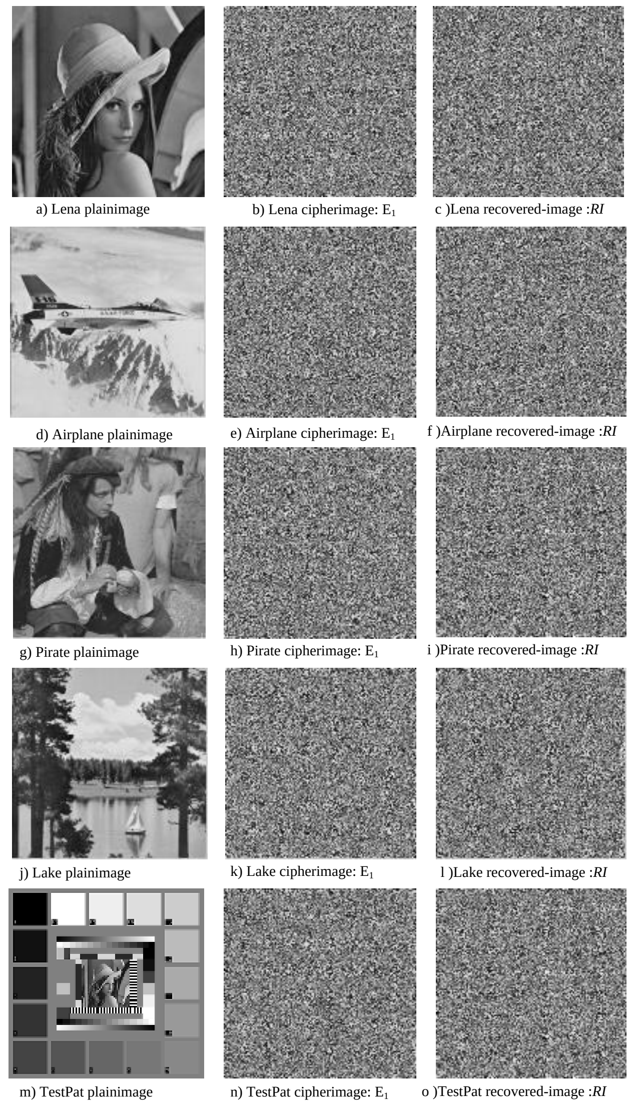

Figure 7: Key sensitivity of the proposed cryptosystem based on wrong decryption key

5.2 Statistical Analysis

By analyzing the histogram of the encrypted images and the adjacent ciphered pixels correlations, we can judge the strength of the suggested cipher to statistical analysis attacks. Accordingly, these tests are applied on the proposed scheme and the obtained results reveal the superior resistance of our cipher against statistical attacks compared to the related ciphers [2, 20, 34, 40, 46]. The tests are thoroughly described in the subsequent two subsections.

5.2.1 Histograms of Encrypted Images

First, an original image of 256 gray levels of size $M \times N$ is encrypted and the histograms of both images (the plainimage and its encryption) are then calculated. The set of five plainimages and their encryption are investigated for this test. The experiment yields the histograms illustrated in Figure 8.

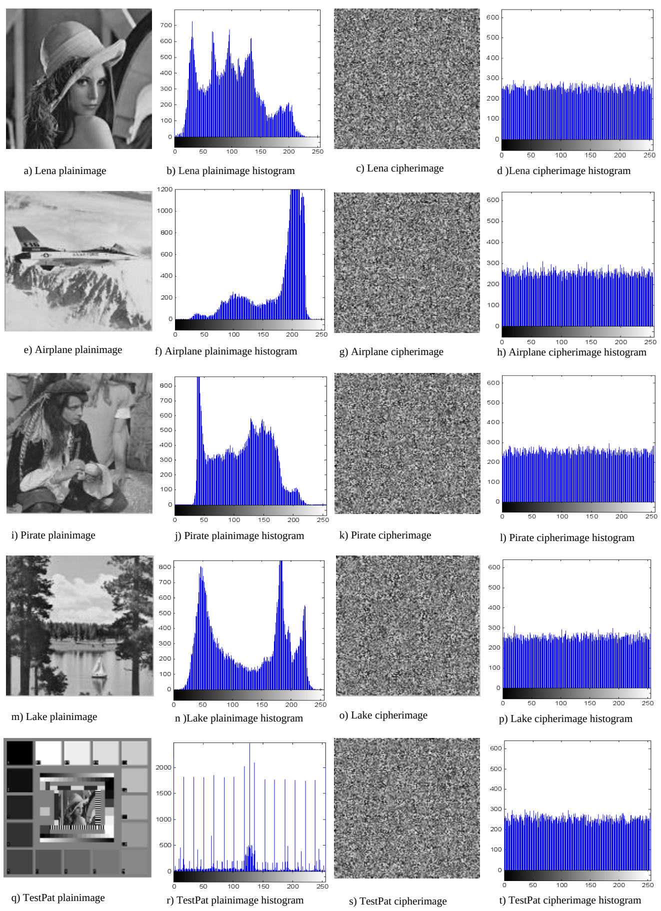

Figure 8: Histogram analysis of the suggested image cipher

Clearly, the histograms of the encrypted images are approximately uniform and are notably distinct from that of the corresponding plainimages. Further, it proves that the suggested cryptosystem has complicated the dependence of the cipherimages statistics on the plainimages statistics and has succeeded in concealing all characters of the plainimages. Furthermore, to statistically demonstrate the histogram uniformity of the cipherimages, the Chi-square test is performed on each cipherimage of the five plainimages in Figure 4. The Chi-square value can be computed according to Equation (27) [3, 10]. Table 8 illustrates the results produced by applying Chi-square test with a significant level 0.05 on the cipherimages obtained from the proposed cipher, Xu *et al.* [40], Cao *et al.* [2], Zhang and Wang [46], Wang *et al.* [34], and Liu *et al.* [20] ciphers. Notably, the proposed cryptosystem always yields a smaller value than the expected value of Chi-square test (293 for a significant level 0.05) which is a good indicator to the uniformity of histograms of the underlying cipherimages. Additionally, the Chi-square test demonstrates that the suggested cipher outperforms the underlying ciphers offered in [2, 20, 34, 40, 46] because it results in the smallest average Chi-square value.

$$\chi^2_{test} = \sum_{s=0}^{H-1} \frac{(O(s) - E(s))^2}{E(s)} \qquad (27)$$

where H, $O(s)$, and $E(s)$ denote the number of image gray levels, the actual and expected occurrences of each gray level, respectively.

Table 8: Chi-square test of the proposed cipher and related current schemes

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	273.81	232.01	343.94	257.96	308.73	231.81
Airplane	244.27	253.30	287.93	275.51	405.94	268.50
Pirate	247.63	274.29	239.95	250.25	675.48	222.20
Lake	266.38	255.93	257.91	278.34	281.80	225.69
TestPat	277.84	272.17	252.71	265.77	50273	228.23
Average	261.99	257.54	276.49	265.57	10388.99	235.29

5.2.2 Correlation of Two Adjacent Pixels

To analyze the correlation of neighboring pixels in the plainimage and the enciphered one, the subsequent steps are performed [3,24]. First, randomly choose a set of pairs of two adjacent pixels from the underlying image along the horizontal (H), the vertical (V), and the diagonal (D) directions. Afterward, estimate the correlation coefficient (CC) between these pairs in each direction. Accordingly, the correlation results for the adjacent pixels in these directions for the encrypted images shown in Figure 4 are examined and compared with the values associated with the ciphers presented in [2, 20, 34, 40, 46]. The results are depicted in Table 9, Table 10, and Table 11. It is obvious that all correlations tend to zero and the proposed cryptosystem produces the smallest average correlation in all directions compared to the other schemes.

Table 9: The correlation of neighboring pixels in H direction

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	0.0069	0.0362	0.0158	0.0156	0.0241	0.0012
Airplane	0.0344	0.0207	0.0213	0.0040	0.0156	0.0100
Pirate	0.0244	0.0063	0.0051	0.0057	0.0074	0.0070
Lake	0.0306	0.0027	0.0110	0.0196	0.0113	0.0042
TestPat	0.0053	0.0153	0.0214	0.0201	0.0243	0.00045
Average	0.0203	0.0162	0.0149	0.013	0.0165	0.00457

Furthermore, Figure 9 represents the distribution of two neighboring pixels in horizontal direction (the same results can be gained for diagonal and vertical adjacent pairs) for the five plainimages and their enciphered images

Table 10: The correlation of neighboring pixels in V direction

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	0.0103	0.0087	0.0115	0.0044	0.0042	0.0023
Airplane	0.0057	0.0061	0.0072	0.0027	0.0063	0.0059
Pirate	0.0096	0.0045	0.0147	0.0022	0.0164	0.0073
Lake	0.0079	0.0120	0.0145	0.0276	0.0118	0.0034
TestPat	0.0297	0.0056	0.0051	0.0048	0.0228	0.0169
Average	0.0126	0.0074	0.0106	0.0083	0.0123	0.0072

Table 11: The correlation of neighboring pixels in D direction

Image	**[40]**	**[2]**	**[46]**	**[34]**	**[20]**	**Ours**
Lena	0.0149	0.0107	0.0240	0.0083	0.0064	0.00025
Airplane	0.0022	0.0128	0.0161	0.0209	0.0077	0.0060
Pirate	0.0054	0.0077	0.0135	0.0453	0.0094	0.0182
Lake	0.0073	0.0209	0.0087	0.0227	0.0241	0.0099
TestPat	0.0136	0.0101	0.0069	0.0240	0.0253	0.0027
Average	0.0087	0.0124	0.0138	0.0242	0.0146	0.00741

shown in Figure 4. Consequently, the obtained results attest that the suggested cryptosystem can remove the tight correlation between neighboring pixels of the plainimage.

5.3 Differential Attacks

Differential attack is an effective methodology to crack the cipher by comparing the encryption results of slightly different plainimages. So, a desirable feature of a good cipher is its sensitive to slight changes (only one bit modification) of the plainimage. To assess the effect of altering only one pixel of the plainimage on the obtained encryption from the proposed scheme, the CC, $NPCR$ and $UACI$ criteria can be exploited [3, 44, 46]. This experiment assumes that I_1 and I_2 be two identical plainimages except for only one pixel and the corresponding encrypted images are denoted by E_1 and E_2. Afterward, the values of CC, $NPCR$ and $UACI$ for E_1 and E_2 are calculated. Several tests are carried out on the proposed cipher to reveal the effect of modifying a single pixel of an image of 256 gray levels. The obtained values are presented in Table 12 and shown in Figure 10. Particularly, the average $NPCR$ is evaluated to be over 99.62% (the expected value of $NPCR$ for two randomly generated images is 99.60% [10] which in turn confirms that the suggested cipher is extremely sensitive to insignificant variations of the original plainimage. Moreover, $UACI$ is estimated to be over 33.54% (the expected value of $UACI$ for two randomly generated images is 33.46% [10] showing thereby that the rate of influence based on a single pixel modification is particularly large. Also, there is a negligible CC value between E_1 and E_2. Briefly, the obtained values for CC, $NPCR$ and $UACI$ demonstrate that the suggested cipher can effectively withstand the differential attacks.

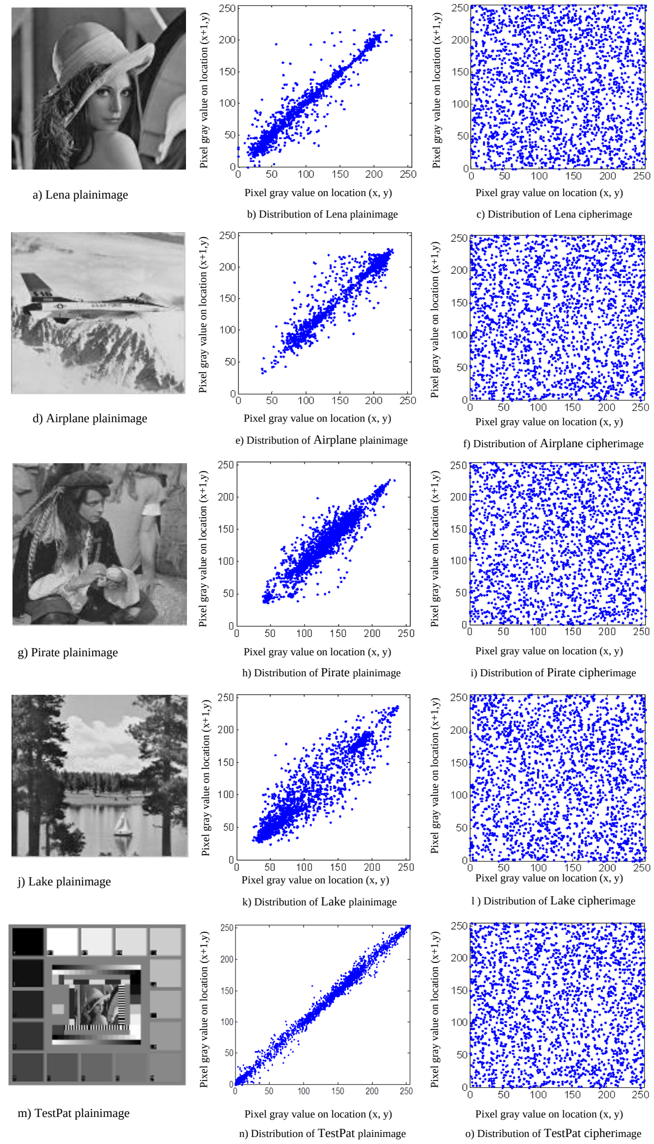

Figure 9: Neighboring pixels correlation analysis of the suggested image cipher

Table 12: Plaintext sensitivity of the suggested cipher

Image	CC	$NPCR(\%)$	$UACI(\%)$
Lena	0.0055	99.6155	33.5859
Airplane	0.0020	99.6207	33.5433
Pirate	0.0051	99.6445	33.4911
Lake	0.0053	99.6170	33.6044
TestPat	0.00046	99.6414	33.5238
Average	0.00367	99.6278	33.5497

6 Conclusions

In this paper, a novel selective bit-level image cryptosystem based on self-adaptive encryption has been suggested. The self-adaptive encryption employs the information extracted from a selected group of image bit-planes to make the encryption result related directly to the plainimage.

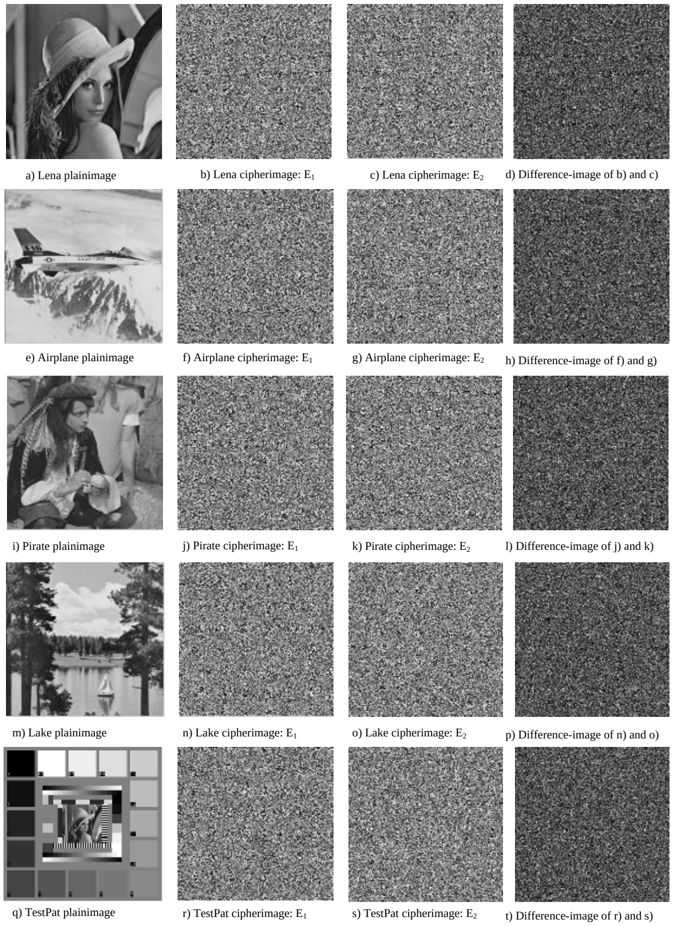

Figure 10: Plainimage sensitivity of the suggested image cipher

Extensive simulations and security analyses have been implemented on the suggested cryptosystem including statistical analysis, key space analysis, secret key and plainimage sensitivity analyses. Accordingly, the obtained results demonstrate that the presented image cipher can perfectly hide the plainimage information and further be suitable for secure image storage and communications.

Acknowledgments

The author gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 1, pp. 136–147, 2013.

[2] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.

[3] J. Chen, Z. Zhu, C. Fu, H. Yu, and Y. Zhang, "Reusing the permutation matrix dynamically for efcient image cryptographic algorithm," *Signal Processing*, vol. 111, pp. 294–307, 2015.

[4] A. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption," *Information Sciences*, vol. 355-356, pp. 314–327, 2015.

[5] C. Fu, B. B. Lin, Y. S. Miao, X. Liu, and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[6] C. Fu, W. H. Meng, Y. F. Zhan, Z. L Zhu, F. C. M. Lau, C. K. Tse, and H. F Ma, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000–1010, 2013.

[7] X. He, Q. Zhu, , and P. Gu, "A new chaos-based encryption method for color image," in *Proceedings of The International Conference on Rough Sets and Knowledge Technology (RSKT 2006)*, pp. 671–678, Chongqing, China, July 2006.

[8] T. Hoang and H. Thanh, "Cryptanalysis and security improvement for a symmetric color image encryption algorithm," *Optik*, vol. 155, pp. 366–383, 2018.

[9] A. Jolfaei and X. Wu, "On the security of permutationonly image encryption schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 235–246, 2016.

[10] H. Kwok and K. Tang, "A fast image encryption system based on chaotic maps with nite precision representation," *Chaos, Solitons Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[11] C. Li, "On the security of a chaos-based encryption method for color image," in *Proceedings of The Third International IEEE Scientific Conference on Physics and Control (PhysCon 2007)*, Potsdam, Germany, September 2007.

[12] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image and Vision Computing*, vol. 29, no. 9, pp. 1371–1381, 2009.

[13] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, 2009.

[14] M. Li, Y. Guo, J. Huang, and Y. Li, "Cryptanalysis of a chaotic image encryption scheme based on permutation-diffusion structure," *Signal Processing: Image Communication*, vol. 62, pp. 164–172, 2018.

[15] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Image Communication*, vol. 23, no. 3, pp. 212–223, 2008.

[16] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238–246, 2017.

[17] S. Lian, *Multimedia content encryption: techniques and applications (1ed)*. USA: CRC Press/Taylor and Francis, 2008.

[18] S. G. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[19] H. J. Liu and X. Y. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 284, no. 16, pp. 3895–3903, 2011.

[20] J. Liu, D. Yang, H. Zhou, and S. Chen, "A digital image encryption algorithm based on bit-planes and an improved logistic map," *Multimedia Tools and Applications*, vol. 77, no. 8, pp. 10217–10233, 2018.

[21] A. Mitra, Y. V. Rao, and S. R. Prasnna, "A new image encryption approach using combinational permutation techniques," *International Journal of Electrical and Computer Engineering*, vol. 1, no. 2, pp. 127–131, 2006.

[22] R. A. Mollin, *An introduction to cryptography (2ed)*. USA: CRC Press, 2006.

[23] B. Norouzi and S. Mirzakuchaki, "Breaking an image encryption algorithm based on the new substitution stage with chaotic functions," *Optik*, vol. 127, no. 14, pp. 5695–5701, 2016.

[24] C. Pak and L. Huang, "A new color image encryption using combination of the 1d chaotic map," *Signal Processing*, vol. 138, pp. 129–137, 2017.

[25] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[26] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, no. 15, pp. 10631–10648, 2016.

[27] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.

[28] L. Teng and X. Y. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Optics Communications*, vol. 285, no. 20, pp. 4048–4054, 2012.

[29] X. Tong and M. Cui, "Image encryption with compound chaotic sequence cipher shifting dynamically," *Image and Vision Computing*, vol. 26, no. 6, pp. 843–850, 2008.

[30] G. Tu, X. Liao, and T. Xiang, "Cryptanalysis of a color image encryption algorithm based on chaos," *Optik*, vol. 124, no. 22, pp. 5411–5415, 2013.

[31] X.-Y. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[32] X.-Y. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[33] X. Y. Wang, X. J Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dynamics*, vol. 63, no. 4, pp. 587–597, 2011.

[34] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using dna sequence operations," *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, 2015.

[35] Z. Wang and A. Bovik, *Modern image quality assessment: Synthesis lectures on image, Video and Multimedia Processing (1ed)*. USA: Morgan and Claypool, 2006.

[36] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, pp. 292–300, 2018.

[37] T. Xiang, K. W. Wong, and X. F. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, 023115, 2007.

[38] W. Xiangjun, K. Haibin, and K. Jrgen, "A new color image encryption scheme based on dna sequences and multiple improved 1d chaotic maps," *Applied Soft Computing*, vol. 37, pp. 24–39, 2015.

[39] D. Xiao, X. F. Liao, and P. C. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[40] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[41] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010.

[42] J. C. Yen and J. I. Guo, "Design of a new signal security system," in *Proceedings of The IEEE International Symposium on Circuits and Systems (ISCAS 2002)*, pp. 121–124, Scottsdale, Ariz, USA, May 2002.

[43] W. Zhang, K. Wong, H. Yu, and Z. Zhu, "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion," *Optics Communications*, vol. 285, no. 9, pp. 2343–2354, 2012.

[44] W. Zhang, K. Wong, H. Yu, and Z. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 3, pp. 584–600, 2013.

[45] W. Zhang, H. Yu, Y. Zhao, and Z. Zhu, "Image encryption based on three dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.

[46] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.

[47] X. Y. Zhao, G. Chen, D. Zhang, X. H. Wang, and G. C. Dong, "Decryption of pure-position permutation algorithms," *Journal of Zhejiang University-SCIENCE A*, vol. 5, no. 7, pp. 803–809, 2004.

[48] Y. Zhou, W. Cao, and C. L. P. Chen, "Image encryption using binary bitplane," *Signal Processing*, vol. 100, pp. 197–207, 2014.

[49] Z. L. Zhu, W. Zhang, K. W Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

Biography

Hossam Diab received his B.S. degree, the M.Sc. degree and Ph.D. degree in Computer Science from Faculty of Science, Menoufia University, Egypt in 1999, 2004 and 2010, respectively. He is an assistant Professor at the Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Egypt. However, he is currently working as a visitor for Computer Science and Engineering College, Taibah University, Saudi Arabia. His research interests are in the areas of cryptography, application of chaotic systems in multimedia content encryption, digital image processing, image compression, image watermarking.