

Colour image encryption based on hybrid bit-level scrambling, ciphering, and public key cryptography

Ahmed Kamil Hasan Al-Ali, Jafaar Mohammed Daif Alkhasraji

Department of Electromechanical Engineering, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Sep 8, 2022

Revised Nov 2, 2022

Accepted Dec 9, 2022

Keywords:

Bit-level scrambling

Hyper-chaotic maps

Image encryption

Pseudo random bit generator

Public key cryptography

ABSTRACT

This paper proposes an image encryption technique using three stages algorithms based on hyper-chaotic maps. In the first scenario, bit-level scrambling (BLS) using a 2D coupled chaotic map (2D-CCM) is used to encrypt the bits of the basic colour image. In the second strategy, the scrambled bit level is XORed with pseudo random bit generator (PRBG). The PRBG is designed using a combination of chaotic maps, including, logistic map (LM), sine map (SM), 5D chaotic map (5D-CM), enhanced quadratic map (EQM), and 2D henon SM (2D-HSM). The public key based on the Chebyshev polynomial chaotic map is used as the final phase of the encryption algorithms. The performance analysis of the proposed image encryption technique is validated through various criteria such as fundamental space analysis, correlation coefficient, entropy, the number of pixels changes rate (NPCR), and unified average-changing intensity (UACI). Also, the obtained results are compared with other recent studies. The simulation results demonstrated that the proposed technique has robust security and it provides the image with high protection against various attacks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ahmed Kamil Hasan Al-Ali

Department of Electromechanical Engineering, University of Technology

Baghdad, Iraq

Email: ahmed.k.alali@uotechnology.edu.iq

1. INTRODUCTION

The development of multimedia technologies and computer networks has made transmitting and sharing data an uncomplicated process through the network [1]. Among these data, is a digital image format. Such a form is widely used because it is capable of carrying much data and it contains confidential besides private personal information [2]. However, because of the transmission and sharing of digital images, a third party could obtain the image or change the data of the original image. Thus, image encryption techniques have an essential role in protecting digital image transmission from attackers. From this perspective, image encryption is the process of transforming the original information image into another kind that is completely different from the original [3]. Although various traditional encryption techniques have been proposed in the literature, for instance, the data cryptography model, and the algorithm such as Rivest-Shamir-Adleman. According to the previous studies, these techniques demonstrated a flaw in the application process of image cryptography because digital images have some essential characteristics, such as a high degree of correlation and redundancy between neighbouring pixels [4], [5]. Furthermore, the security of the image is based on designing the public key cryptosystem. In this context, various public key cryptosystem techniques have been proposed such as knapsack public key [6], public key based on algebraic coding [7], and lattice public key [8]. In this paper, we focus on the Chebyshev polynomial. The Chebyshev polynomial is based on a chaotic

map [9]. To improve the security of the digital image, various techniques have been proposed, such as bit-level permutation [10], deoxyribonucleic acid (DNA) [11], and chaotic systems [12]. It is worth to meeting that most image encryption techniques are based on chaotic systems [13]–[15] because of their high sensitivity to the initial value, ergodicity, and pseudo-randomness. Permutation and diffusion are the two main processes in a chaotic system. These two processes are repeated many times until the perfect security level is obtained. Wherein the permutation is used to remove the high correlation between adjacent pixels. The purpose of diffusion is to modify the values of pixels and this process is obtained using chaotic maps.

The chaotic system can be divided into one-dimensional and high-dimensional chaotic systems. A one-dimensional chaotic system, including a logistic map (LM) [16], 1D sine map (SM) [17], and iteration LM [18], were proposed to improve the performance of image security. One advantage of a one-dimensional chaotic system includes a simple structure and high-efficiency encryption while it suffers from a low level of security. High-dimensional chaotic systems such as 5D chaotic maps (5D-CM) [19], 3D Lorenz mapping [20], and 4D chaotic maps with DNA [21]. Although the high-dimensional chaotic maps improve image security performance, the encryption time of the high-dimensional chaotic systems is long due to their difficult implementation structure [2].

The contribution of this paper is to encrypt the colour images with high levels of security using hyperchaotic systems in three scenarios. In the first stage, bit-level scrambling (BLS) is used, where the index permutation is designed using 2D coupled chaotic map (2D-CCM). In the second phase, the stream cipher system with the pseudo random bit generator (PRBG) is designed using multi random keys, where each key is generated using chaotic maps, including LM, SM, 5D-CM, enhanced quadratic map (EQM), and 2D henon SM (2D-HSM). A public key based on the Chebyshev polynomial map is applied in the last step of encryption. Different intelligibility measurements were used to test the quality of the encrypted colour images, including correlation coefficient, entropy, number of pixels changes rate (NPCR), unified average changing intensity (UACI), and histogram analysis.

This paper is organized as follows. In section 2, method is introduced. Pseudo-random bit generation using hyper-chaotic maps is presented in section 3. The fourth section describes the hybrid image encryption scheme structure. The hybrid image decryption system structure is illustrated in section 5. Experimental results are presented in section 6. The key sensitivity analysis is presented in section 7, finally, the conclusion is depicted in section 8.

2. METHOD

This section presents different types of chaotic maps. These chaotic maps are used to generate the index permutation and PRBG. We will employ eight chaotic map formulas for investigation purpose. A detailed description of chaotic maps is presented in the following subsections..

2.1. Logistic map

The LM can determine as [22]:

$$z_{i+1} = 4\rho z_i(1 - z_i) \quad (1)$$

where ρ is the control factor and it values between 0.89 to 1.

2.2. Sine map

The SM is a one-dimensional chaotic map and it can determine as [22]:

$$z_{i+1} = \rho \sin(\pi z_i) \quad (2)$$

where ρ is the control parameter and it values between 0.87 to 1.

2.3. 5D chaotic map

The 5D-CM is obtained by combining 3D Lorenz and LMs and it can be defined as [19]:

$$\begin{aligned} Z_{i+1} &= a Z_i(1 - Z_i) \\ R_{i+1} &= b R_i S_i - c W_i \\ S_{i+1} &= Z_i + R_i \\ U_{i+1} &= R_i + d W_i \\ W_{i+1} &= S_i + Z_i U_i \end{aligned} \quad (3)$$

where Z_i, R_i, S_i, U_i , and W_i are state variables of the system, a, b, c , and d are system parameters. The values of a, b, c , and d are 4, 0.5, 0.3, and 0.9, respectively. The initial values of $Z(0)=0.9, R(0)=-0.28, S(0)=0.183, U(0)=0.5$, and $W(0)=0.57$.

2.4. 2D coupled chaotic map

The 2D-CCM can be defined as [23]:

$$\begin{aligned} Z_{i+1} &= \sin\left(\frac{k}{\sin(R_i)}\right) \\ R_{i+1} &= \gamma \sin(\pi(Z_i + R_i)) \end{aligned} \quad (4)$$

where the control parameter $k \neq 0, \gamma \in (0,1]$, and the initial value of $R_0 \neq 0$.

2.5. Enhanced quadratic map

The EQM can be represented mathematically as [15]:

$$Z_{i+1} = \left(r - 2^5 (r - Z_i^2)^2 \right) \bmod 1 \quad (5)$$

where $r \in [0.05, 4]$.

2.6. 2D hyper-chaotic map

The 2D-HCM can be defined as [24]:

$$\begin{aligned} Z_{i+1} &= a_1 + a_2 Z_i + a_3 R_i \\ R_{i+1} &= b_1 + b_2 Z_i^2 \end{aligned} \quad (6)$$

where $a_1 = 0.2, a_2 = 0.3, a_3 = 0.5, b_1 = -1.7$, and $b_2 = 3.7$.

2.7. 2D henon sine map

The 2D-HSM is defined as [25]:

$$\begin{aligned} Z_{i+1} &= (1 - a \sin^2(Z_i + R_i)) \bmod 1 \\ R_{i+1} &= b Z_i \bmod 1 \end{aligned} \quad (7)$$

2.8. Chebyshev polynomial

The Chebyshev polynomial is defined as [26]:

$$T_n(x) = (2x T_{n-1}(x) - T_{n-2}(x)) \bmod N \quad (8)$$

where $T_0(x) = 1, T_1(x) = x$, and N is the total number of pixels in image. The value of Chebyshev polynomial ($T_n(x)$) is between -1 to 1. The semigroup property is one of the most essential properties of the Chebyshev polynomial and it is used for the construction of the public key. The semigroup property is defined as:

$$T_s(T_r(x) \bmod N) \bmod N = T_r(T_s(x) \bmod N) \bmod N \quad (9)$$

The commute under composition is a property of Chebyshev polynomial and it can be defined as:

$$T_s(T_r(x) \bmod N) \bmod N = T_{sr} \bmod N \quad (10)$$

3. PSEUDO RANDOM BIT GENERATOR (PRBG) BASED ON HYBRID CHAOTIC MAPS

Figure 1 shows the proposed PRBG based on a one, two, and five-dimensional chaotic map. Six PRBGs are produced in the first using a hyperchaotic map and then the final key is generated by XORed these keys according to:

$$PRBG_i = K_1(i) \oplus K_2(i) \oplus K_3(i) \oplus K_4(i) \oplus K_5(i) \oplus K_6(i), \quad i = 1, 2, \dots, 8MN \quad (11)$$

where $K_1 K_2 K_3 K_4 K_5$ and K_6 are the PRBG based on LM, SM, EGM, 2D-HCM, 2D-HSM, and 5D-CM, respectively. The key space for each key is summarized as: LM (x_0, ρ, y_0, ρ) , SM (x_0, ρ, y_0, ρ) , EQM (x_0, r, y_0, r) , 2D-HCM $(x_0, y_0, a_1, a_2, a_3, b_1, b_2)$, 2D-HSM (x_0, y_0, a, b) , and 5D-CM $(Z_0, R_0, S_0, W_0, U_0, a, b, c, d)$. Therefore, there are 32 variables used as a key space to generate PRBG.

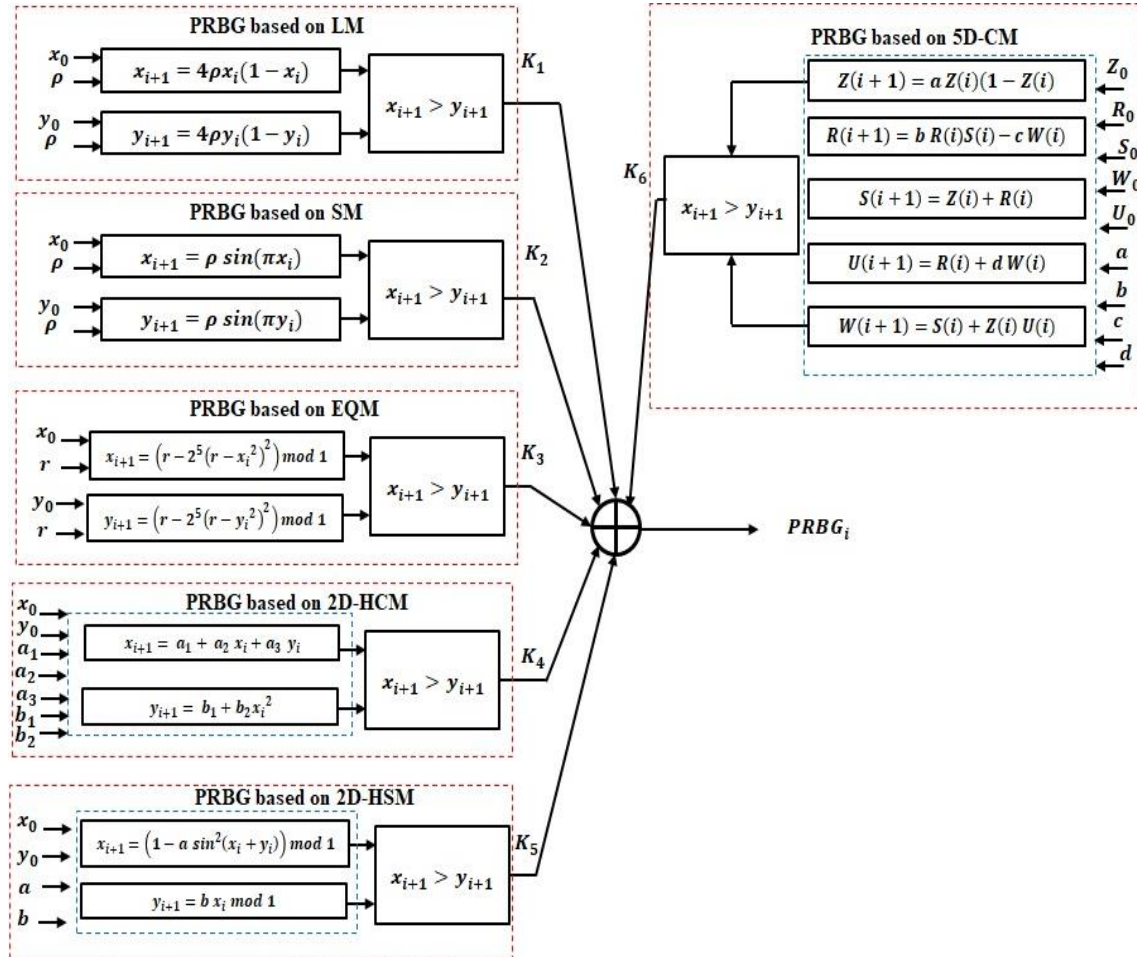


Figure 1. The proposed PRBG based on hyperchaotic maps

4. HYBRID IMAGE ENCRYPTION SYSTEM STRUCTURE

Figure 2 shows the proposed image encryption system using three sequential algorithms adopted in this investigation. The first step of the encryption procedure is the implementation of a bit-level scrambling algorithm to shuffle the bits of the channel image; the next step is the encryption process using the XOR ciphering system. Finally, public key cryptography algorithms on the transmitter side were applied to the output stream bits of the ciphering matrix. A more detailed description of each stage is presented in the following subsections.

4.1. Bit-level scrambling algorithm (stage one)

The first stage of the encryption process is a BLS algorithm that is used to shuffle the bits of the channel image (red (R) or green (G) or blue (B) channel) according to the permutation index generated using the 2D-CCM as described in subsection (2.4). Each channel matrix has the size. The exhaustive explication of the bit-level-scrambling procedures is depicted in Algorithm 1. This algorithm is applied for each channel with its initial conditions and produced the permuted binary matrix $S(j, i)$, $j=\{1 R, 2 G, \text{ and } 3 B\}$, $i=1$ to $8 MN$. The BLS algorithm required four keys representing the initial conditions of 2D-CCM (k, R_0, Z_0) for each channel.

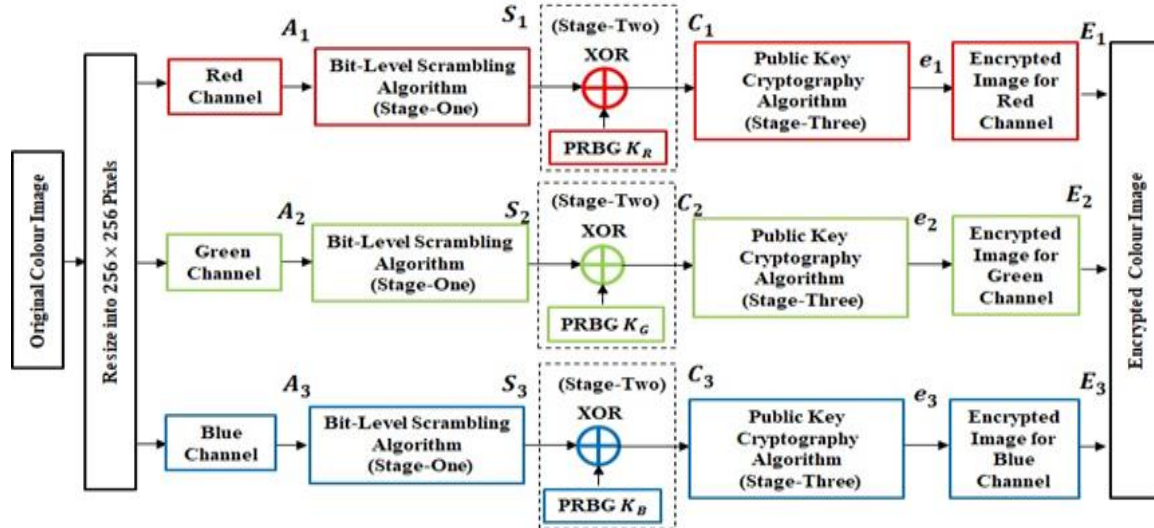


Figure 2. Proposed image encryption system

Algorithm 1. BLS algorithm

Input: Plain Image $A \in \mathbb{R}^{3 \times M \times N}$, k_j , γ_j , R_{0j} , Z_{0j} , $j=1,2,3$.

Output: Permuted Sequence, $S \in \{0,1\}$ of size $3 \times 8MN$

Step 1: Reshape $A_{3 \times M \times N}$ to $A_{3 \times MN}$.

Step 2: Convert A to binary stream vector, $b_j = \{b_{j,1}, b_{j,2}, \dots, b_{j,8MN}\}$.

Step 3: For $j=1$ to 3 Compute

For $i=1$ to $8 \times M \times N - 1$, Compute

$$Z_{j,i+1} = \sin\left(\frac{k_j}{\sin(R_{j,i})}\right)$$

$$R_{j,i+1} = \gamma_j \sin(\pi(Z_{j,i} + R_{j,i}))$$

End For

End For

Step 4: $[\sim PIj] = \text{sort}(Z_j)$.

Step 5: For $j=1$ to 3 Compute

For $i = 1$ to $8 \times M \times N$, compute

$$S(j, i) = b(1, PIj(i))$$

End For

End For

4.2. XOR ciphering system (stage two)

The second step of encryption is XOR Ciphering system in which the j^{th} channel and i^{th} bit of $S(j, i)$ ($j=1, 2, 3$ and $i=1, \dots, 8MN$) is XORed with PRBG key, PRBG (j, i) ($K_R(i) = \text{PRBG}(1, i)$, $K_G(i) = \text{PRBG}(2, i)$, $K_B(i) = \text{PRBG}(3, i)$, $i=1, \dots, 8MN$). Correspond for j^{th} channel and produced the j^{th} ciphered message $C(j, i)$ according to:

$$C(j, i) = S(j, i) \oplus \text{PRBG}(j, i) \quad (12)$$

where \oplus is XOR bitwise operation. The j^{th} stream binary keys, PRBG (j, i), $j=1, 2, 3$, $i=1, \dots, 8MN$ are generated using PRBG which is described in section (3), where each channel has self-initial conditions.

4.3. Public key cryptography encryption algorithm (stage three)

This section presents public key cryptography encryption algorithm. Algorithm 2 shows the third stage public key cryptography encryption algorithm at the transmitter side. The algorithm of public key cryptography encryption is applied to the output stream bits of the ciphering matrix $C(j, i)$. The objective is to produce the encrypted color image $E(j, n, m)$, $j=1, 2, 3$, $n=1, \dots, N$, $m=1, \dots, M$.

Algorithm 2. Public key cryptography encryption algorithm

Input: $C(j, i) \in \{0,1\}$, $j=1,2,3$, $i=1,2,\dots,8NM$, large number Q , $\alpha < Q$, secret

keys s_j , $j=1,2,3$

Output: $E(j, n, m) \in \mathbb{R}^{3 \times N \times M}$, $j=1,2,3$, $n=1,2,\dots,N$, $m=1,2,\dots,M$.

Step 1: Compute $q = \log_2(Q)$

Step 2: Reshape $C^{3 \times 8NM}$ to $C_f^{3 \times \beta \times q}$, $\beta = 8NM/q$.

Step 3: Convert q bits in C_r from binary to decimal $C_d^{3 \times \beta}$
Step 4: Compute $\Gamma_j = T_{s_j}(\alpha) \bmod Q$, $j=1,2,3$
Step 5: For $j=1$ to 3 Compute
 For $t=1$ to β Compute
 $e(j,t) = C_d(j,t) \Gamma_j \bmod Q$
 End For
 End For
Step 6: Convert $e^{3 \times \beta}$ to binary number $B^{3 \times \beta \times q}$
Step 7: Reshape $B^{3 \times \beta \times q}$ to $B^{3 \times N \times M \times 8}$
Step 8: Convert to decimal number $E^{3 \times N \times M}$

5. HYBRID IMAGE ENCRYPTION SYSTEM STRUCTURE

Figure 3 shows the proposed image decryption system. The proposed system consists of three stages of the algorithms. The first stage is the public key cryptography decryption algorithms, the second deciphering and the third stage is bit-level descrambling (BDS) algorithms. A detailed description of each stage is presented in the following subsections.

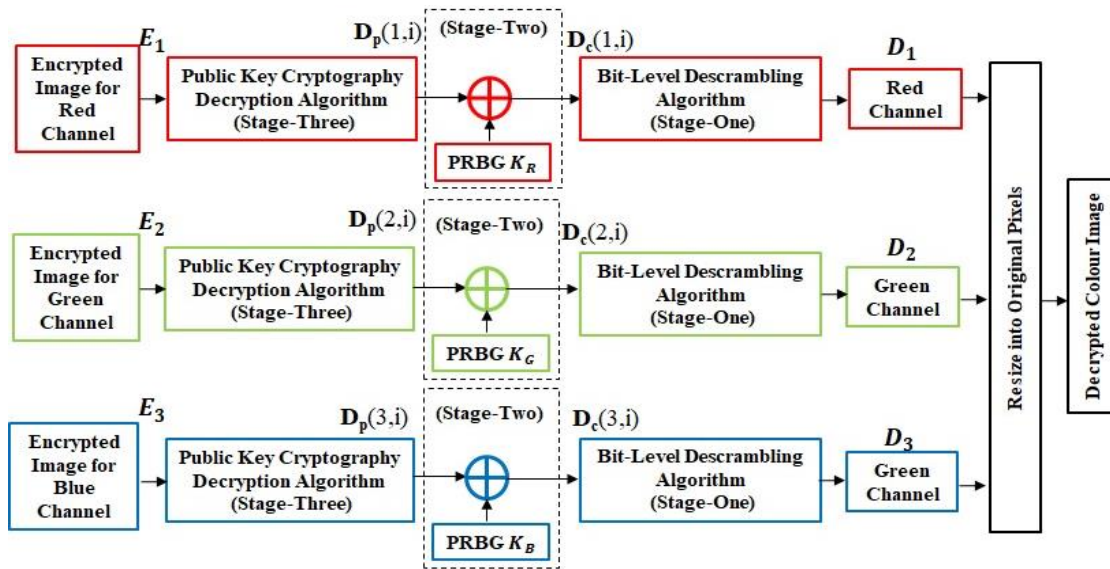


Figure 3. Proposed image decryption system

5.1. Public key cryptography encryption algorithm (stage three)

This section presents public key cryptography encryption algorithm. Algorithm 3 shows the third stage public key cryptography decryption algorithm at the reception side. The public key cryptography decryption algorithm is applied to the encrypted colour matrix $E^{3 \times N \times M}$ to produce the sequence $D_p(j, i)$, $j=1, 2, 3, i=1, \dots, 8NM$.

Algorithm 3. Public key cryptography decryption algorithm

Input: $E(j, n, m) \in \{0,1\}$, $j=1,2,3$, $n=1,2,\dots,N$, $m=1,\dots,M$, large number Q , $\alpha < Q$, secret keys r_j , $j=1,2,3$

Output: $D_p(j, i) \in \mathbb{R}^{3 \times 8NM}$, $j=1,2,3$, $i=1,2,\dots,8NM$.

Step 1: Compute $q = \log_2(Q)$

Step 2: Reshape $E^{3 \times N \times M}$ to $D_f^{3 \times \beta \times q}$, $\beta = 8NM/q$.

Step 3: Convert q bits in D_f from binary to decimal $D_d^{3 \times \beta}$

Step 4: Compute $\Gamma_j = T_{r_j}(\alpha) \bmod Q$, $j=1, 2, 3$

Step 5: For $j=1$ to 3 Compute

 For $t=1$ to β Compute

$d(j, t) = D_d(j, t) / \Gamma_j \bmod Q$

 End For

End For

Step 6: Convert $d^{3 \times \beta}$ to binary number $B^{3 \times \beta \times q}$

Step 7: Reshape $B^{3 \times \beta \times q}$ to $D_p^{3 \times 8MN}$

5.2. XOR deciphering system (stage two)

The second stage of decryption is XOR Deciphering system in which the j^{th} channel and i^{th} bit of $D_p(j, i)$ ($j=1, 2, 3$ and $i=1, \dots, 8MN$) is XORed with PRBG key, $\text{PRBG}(j, i)$ $K_R(i) = \text{PRBG}(1, i)$, $K_G(i) = \text{PRBG}(2, i)$, $K_B(i) = \text{PRBG}(3, i)$, $i=1, \dots, 8MN$). Correspond for each j^{th} channel and produced the j^{th} deciphered message $D_c(j, i)$ according to:

$$D_c(j, i) = D_p(j, i) \oplus \text{PRBG}(j, i) \quad (13)$$

where \oplus is XOR bitwise operation. The j^{th} stream binary keys, $\text{PRBG}(j, i)$, $j=1, 2, 3$, $i=1, \dots, 8MN$ are generated using PRBG which is described in section 3, where each channel has self-initial conditions. We assume that the synchronization between the keys at the transmitter and receiver is established.

5.3. Bit-level descrambling algorithm (stage one)

The last stage of the decryption process is the BDS algorithm that is used to disorganize the information of the channel image pursuant to the permutation index yielded using the 2D-CCM as described in subsection 2.4. The exhaustive explication of the BDS procedures is depicted in Algorithm 4. This algorithm is applied for each channel with its initial conditions and produces the original decrypted colour matrix. As for the transmitter side, the BDS algorithm required four keys representing the initial conditions of 2D-CCM (k, R_0, Z_0) for each channel.

Algorithm 4. BLD algorithm

Input: The matrix $D_c \in \text{Binary}^{3 \times 8MN}$, k_j , γ_j , $R_{0,j}, Z_{0,j}$, $j=1, 2, 3$.

Output: Decrypted colour image, $D \in \mathbb{R}^{3 \times N \times M}$.

Step 1: For $j=1$ to 3 Compute
For $i=1$ to $8 \times M \times N - 1$, Compute

$$Z_{j,i+1} = \sin\left(\frac{k_j}{\sin(R_{j,i})}\right)$$

$$R_{j,i+1} = \gamma \sin(\pi(Z_{j,i} + R_{j,i}))$$

End For

End For

Step 4: $[\sim \text{PI}_j] = \text{sort}(Z_j)$.

Step 5: For $j=1$ to 3 Compute

For $i = 1$ to $8 \times M \times N$, compute

$$D_l(j, \text{PI}_j(i)) = D_c(1, i)$$

End For

End For

Step 6: Reshape $D_l^{3 \times 8MN}$ to $D_l^{3 \times N \times M \times 8}$

Step 7: Convert to 8 bits binary to Decimal $D^{3 \times N \times M}$

6. EXPERIENTIAL RESULTS

Three standard colour images, including (Lena, Peppers, and Barbara) are used as input images to ensure the efficiency of the proposed image encryption technique. Figure 4 shows the simulation findings of the new image cryptography method. Figures 4(a) and (b) show the original images and histogram of the original images, respectively. Figure 4(c) and (d) show the cipher images and histogram of cipher images, respectively. The decrypted images are shown in Figure 4(e). It can be noted that the cipher images are no valid information and the decrypted images are similar to the plain images. Also, it can be seen from Figures 4(b) and (d) that the histogram of the cipher images is unlike that of the plain images and the histogram of the cipher images is close to the uniform distribution. The simulation results demonstrate that the proposed technique is secure.

6.1. Key space

The size of the key space is determined by multiplying the key for each parameter and initial condition. The security level of image encryption improves when the number of key spaces is increased. Large key size is more robust against brute-force attacks that must exceed 2^{100} [14], [19], [22]. In this paper, the following parameters and initial condition: 2D-CCM ($Z(0)$, $R(0)$, k, γ), LM (x_0, ρ, y_0, ρ), SM (x_0, ρ, y_0, ρ), EQM (x_0, r, y_0, r), 2D-HCM ($x_0, y_0, a_1, a_2, a_3, b_1, b_2$), 2D-HSM (x_0, y_0, a, b), and 5D-CM ($Z_0, R_0, S_0, W_0, U_0, a, b, c, d$), and public key cryptography (s_1, s_2, s_3). Therefore, there are 39 keys with a precision 10^{-15} and the total key space is $(10^{15})^{39} \approx 2^{1911}$. Thus, the suggested image cryptography approach is robust against brute-force attacks.

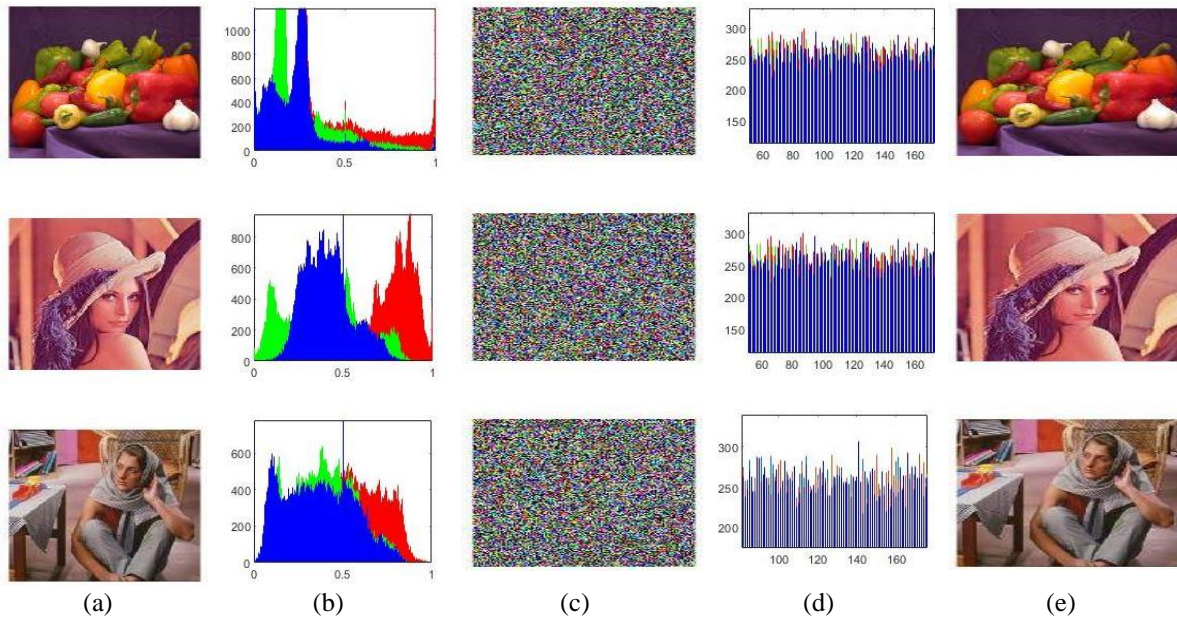


Figure 4. The results of the proposed cryptography technique based on simulation: (a) plain images, (b) histogram of plain images, (c) cipher images, (d) histogram of cipher image, and (e) decrypted images

6.2. Correlation coefficients

The correlation coefficient is a statistical measurement of the relationship between adjacent pixels. In the plain image, the value of the correlation coefficient should be high in the horizontal, vertical, and diagonal directions. Conversely, the correlation coefficient value of the cipher image should be closer to zero. The (14)-(17) of the correlation coefficient between adjacent pixels [27].

$$\rho_{xy} = \frac{\text{covar}(x,y)}{\sqrt{\text{var}(x)\text{var}(y)}} \quad (14)$$

$$E(x) = \frac{1}{T} \sum_{i=1}^T x_i \quad (15)$$

$$\text{var}(x) = \frac{1}{T} \sum_{i=1}^T (x_i - E(x))^2 \quad (16)$$

$$\text{covar}(x,y) = \frac{1}{T} \sum_{i=1}^T (x_i - E(x))(y_i - E(y)) \quad (17)$$

where ρ_{xy} denotes the correlation coefficient between adjacent pixels (x , and y). T stand for the total number of pixels selected from the image. $E(x)$, and $\text{var}(x)$ represent the mean and variance of x , respectively.

Table 1 shows the correlation coefficients of the proposed method using three colour images. It can be seen that the correlation coefficients of cipher images are close to zero, which demonstrates that the suggested image cryptography is an effective approach for reducing the interconnection between neighbouring pixels. Table 2 shows a comparison of the correlation coefficient with other image encryption techniques using Lena image. The results show that the proposed image encryption achieves almost the best results compared with other recent works.

6.3. Entropy

Entropy is widely used to measure the uncertainty of a random variable. The entropy can be defined as [1]:

$$H(x_i) = -\sum_{i=1}^{256} P(x_i) \log_2(P(x_i)) \quad (18)$$

where $P(x_i)$ is the probability of x_i .

For cipher image, the value of entropy should be ideally close to 8 [28]. Table 3 shows the information entropy of the proposed algorithm using three cipher colour images. The outcomes demonstrate that the values of entropy for three cipher image are close to 8, which indicate that cipher image pixels are

uniformly distributed [28]. Table 4 shows a comparison of the information entropy of the proposed algorithm with other image encryption techniques using the Lena image. It can be seen that the values of entropy of the proposed image encryption technique tend to 8, which proves that the suggested approach has strong protection and that a third party can scarcely find useful information from a cipher image.

Table 1. Correlation coefficient of the proposed method using three colour images

Images	Channel	Horizontal		Vertical		Diagonal	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Lena	Red	0.9621	0.0782	0.9923	-0.0097	0.8981	0.0800
	Green	0.9687	-0.0660	0.9884	0.0210	0.8913	-0.1045
	Blue	0.9295	-0.0177	0.9647	-0.0349	0.7729	-0.0080
Peppers	Red	0.8804	-0.0025	0.9831	-0.0951	0.9816	-0.0183
	Green	0.8867	0.0991	0.9870	-0.0608	0.9784	-0.0843
	Blue	0.8486	0.0609	0.9900	-0.1298	0.9065	-0.0673
Barbara	Red	0.9342	-0.0410	0.8977	0.0126	0.9308	-0.0878
	Green	0.8771	0.0592	0.9254	-0.0436	0.9206	0.0291
	Blue	0.8818	0.0639	0.9557	-0.1453	0.9240	-0.0951

Table 2. Comparison of the correlation coefficient with other image encryption techniques using Lena image

Methods	Channel	Horizontal		Vertical		Diagonal	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Ours	Red	0.9621	0.0782	0.9923	-0.0097	0.8981	0.0800
	Green	0.9687	-0.0660	0.9884	0.0210	0.8913	-0.1045
	Blue	0.9295	-0.0177	0.9647	-0.0349	0.7729	-0.0080
[29]	Red	0.9813	0.0092	0.9803	0.0203	0.9668	-0.0073
	Green	0.9691	0.0002	0.9594	-0.0025	0.9433	-0.0131
	Blue	0.9455	0.0076	0.9294	0.0006	0.9099	0.0111
[30]	Red	0.9777	0.0090	0.9508	-0.0027	0.9259	-0.0013
	Green	0.9670	-0.0013	0.9370	-0.0051	0.9111	-0.0155
	Blue	0.9496	-0.0025	0.9171	-0.0103	0.8867	-0.0078
[31]	Red	0.9775	-0.0021	0.9880	0.0027	0.9737	-0.00032
	Green	0.9662	0.0017	0.9817	0.0023	0.9605	0.0010
	Blue	0.9304	0.0012	0.9568	-0.0011	0.9219	0.00069

Table 3. The information theory of the proposed algorithm using three cipher colour images

Images	Channels	Proposed
Lena	Red	7.9981
	Green	7.9980
	Blue	7.9979
Peppers	Red	7.9971
	Green	7.9979
	Blue	7.9978
Barbara	Red	7.9980
	Green	7.9976
	Blue	7.9979

Table 4. Comparability of data entropy of the proposed algorithm with other image encryption techniques using Lena image

Methods	Channels	Proposed
Ours	Red	7.9981
	Green	7.9980
	Blue	7.9979
[23]	Red	7.9912
	Green	7.9913
	Blue	7.9914
[29]	Red	7.9980
	Green	7.9979
	Blue	7.9978
[32]	Red	7.9895
	Green	7.9894
	Blue	7.9894
[33]	Red	7.9966
	Green	7.9972
	Blue	7.9967

6.4. Peak signal to noise ratio

The (19) of peak signal to noise ratio (PSNR) can be represented as [1]:

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N [I(i,j) - C(i,j)]^2} \quad (19)$$

where I is the original plain image and c is the encrypted or decrypted image. Table 5 shows the PSNR tests for different images in case of encryption and decryption. In this table, it can be noticed that low power can be obtained from the encrypted image compared with the decrypted image, proving the validity and robustness of the proposed method.

Table 5. PSNR test for encrypted and decrypted images based on the proposed method

Image	PSNR for encrypted image	PSNR for decrypted image
Lenna	9.5857	52.81
Peppers	7.7337	19.67
Barbara	8.495	34.65

6.5. Differential attack

The NPCR and unified average-changing intensity (UACI) are two essential parameters to determine the differential attack. The NPCR and UACI can be calculated according to the following equations [34]:

$$NPCR = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100 \quad (19)$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times 100 \quad (20)$$

where c_1 and c_2 are two images whose size of $M \times N$. If $c_1(i,j) = c_2(i,j)$, then $D(i,j) = 0$. Otherwise $D(i,j) = 1$. The ideal value of NPCR is 0.996 and UACI is 0.334 [35]. Table 6 shows a comparison of NPCR and UACI for the proposed algorithm using different colour images. It is clear that the quantities of NPCR and UACI are near to the ideal quantities. Table 7 shows a comparison of NPCR and UACI of the suggested algorithm with other image cryptography techniques using Lena's image. The results demonstrate that the proposed image encryption technique is close to ideal values and that our proposed image encryption is more robust to differential attacks.

Table 6. A comparison of NPCR and UACI of the proposed algorithm using different colour images

Images	Channels	NPCR (%)	UACI (%)
Lena	Red	99.6724	33.4985
	Green	99.6992	33.4562
	Blue	99.6682	33.5086
Peppers	Red	99.7853	33.3946
	Green	99.7838	33.5541
	Blue	99.6877	33.3252
Barbara	Red	99.6917	33.6271
	Green	99.6544	33.4530
	Blue	99.6785	33.5630

Table 7. A comparison of NPCR and UACI of the suggested algorithm with other image cryptography techniques using Lena image

Methods	Channels	Channels	UACI (%)
Ours	Red	99.6724	33.4985
	Green	99.6992	33.4562
	Blue	99.6682	33.5086
[23]	Red	99.6243	33.4686
	Green	99.6433	33.5020
	Blue	99.6029	33.4155
[36]	Red	99.6479	33.4390
	Green	99.6579	33.4799
	Blue	99.6288	33.4833
[35]	Red	99.6531	33.4572
	Green	99.6522	33.4715
	Blue	99.6518	33.4384
[32]	Red	99.6052	33.4280
	Green	99.6060	33.4966
	Blue	99.6113	33.3779

6.6. Anti-shear attack

The analysis of anti-shear attack for the proposed method is shown in Figure 5. Figure 5(a) illustrates the original encrypted image. To check the ability of the anti-shear attack for the proposed algorithm, the encrypted image is cut-off by 40×40 in the middle and replacing the cut-off pixels by zero values, as illustrated in Figure 5(b). Figure 5(c) illustrates the decrypted image of the original encrypted image. The decrypted cut image is illustrated in Figure 5(d). In comparison, the results demonstrated that only pixels cut from the encrypted image were affected and the remaining decrypted image has not changed by the cutting.

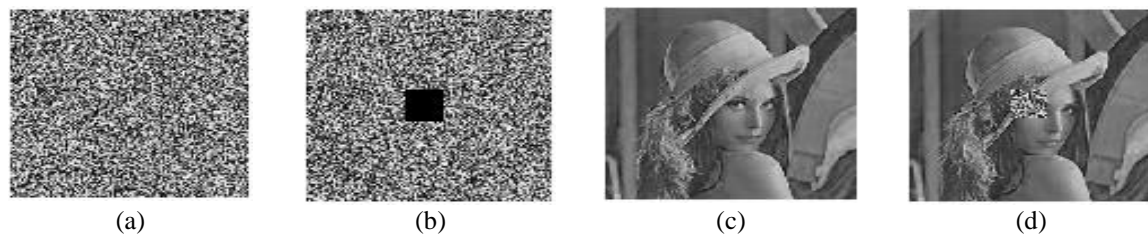


Figure 5. The analysis of the anti-shear attack (a) before cutting, (b) after cutting, (c) decryption before cutting, and (d) decrypting after cutting

7. KEY SENSITIVITY ANALYSIS

A slight modification in the key will have a significant impact on the ciphertext; such a definition is known as key sensitivity. In this context, this experiment used different images and which were given by the first level of the initial key ($K_{4(0)} = [0.234545, 0.98791245]$), and sensitivity key ($K_{4(1)} = [0.2345450000000001, 0.98791245]$) for 2D-HCM. Table 8 shows key sensitivity of the proposed algorithm for different images. It can be seen that the suggested algorithm has outstanding PSNR values besides the entropy measures, confirming that the proposed algorithm has adequate key sensitivity.

Table 8. Key sensitivity analysis for different images

Image	PSNR of decrypted image	PSNR of decrypted image with key sensitivity	Entropy of decrypted image	Entropy of decrypted image with key sensitivity
Lenna	52.81	9.5469	7.0994	7.9969
Barbara	34.00	8.5065	7.5505	7.997
Peppers	19.07	7.7245	7.2181	7.998

8. CONCLUSION

The transmission of images represents an important issue in network security. Attackers could obtain transmitted images through the network. Therefore, it is important to employ a robust image encryption technique to secure transmitted images. In this paper, we proposed an image encryption technique based on hyperchaotic maps based on three scenarios. Firstly, the plain image is permuted using the 2D-CCM. Then, the scrambled image is XORed with a pseudo-random bit generator. The pseudo-random bit generator was designed using a hybrid of chaotic maps. Also, the public key Chebyshev polynomial was applied as the final stage of encryption. Simulation findings demonstrated the validity of the suggested image encryption technique in transforming the plain image into indistinguishable noise ones. The security results show that the suggested method can combat different varieties of offensives. In future work, we will apply DNA coding and anti-noise attack analysis with the proposed image encryption technology to further enhance and investigate the performance of image encryption systems.




REFERENCES

- [1] A. A. Karawia and Y. A. Elmasry, "New encryption algorithm using bit-level permutation and non-invertible chaotic map," *IEEE Access*, vol. 9, pp. 101357–101368, 2021, doi: 10.1109/ACCESS.2021.3096995.
- [2] J. Zheng and T. Lv, "Image encryption algorithm based on cascaded chaotic map and improved Zigzag transform," *IET Image Processing*, vol. 16, no. 14, pp. 3863–3875, Dec. 2022, doi: 10.1049/ipr2.12600.
- [3] M. A. Mokhtar, N. M. Sadek, and A. G. Mohamed, "Design of image encryption algorithm based on different chaotic mapping," in *2017 34th National Radio Science Conference (NRSC)*, Mar. 2017, pp. 197–204, doi: 10.1109/NRSC.2017.7893504.
- [4] H. Xiang and L. Liu, "An improved digital logistic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 79, no. 41, pp. 30329–30355, Nov. 2020, doi: 10.1007/s11042-020-09595-x.




Colour image encryption based on hybrid bit-level scrambling, ciphering ... (Ahmed Kamil Hasan Al-Ali)

- [5] S. K.U. and A. Mohamed, "A novel image encryption scheme using both pixel level and bit level permutation with chaotic map," *Applied Soft Computing*, vol. 90, pp. 1–17, May 2020, doi: 10.1016/j.asoc.2020.106162.
- [6] M. S. Lee, "Improved cryptanalysis of a knapsack-based probabilistic encryption scheme," *Information Sciences*, vol. 222, pp. 779–783, Feb. 2013, doi: 10.1016/j.ins.2012.07.063.
- [7] H. Fujita, "Quantum McEliece public-key cryptosystem," *Quantum Information and Computation*, vol. 12, no. 3–4, pp. 181–203, Mar. 2012, doi: 10.26421/QIC12.3-4-1.
- [8] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2012, pp. 738–755, doi: 10.1007/978-3-642-29011-4_43.
- [9] L. Kocarev, J. Makraduli, and P. Amato, "Public-key encryption based on Chebyshev polynomials," *Circuits, Systems and Signal Processing*, vol. 24, no. 5, pp. 497–517, Oct. 2005, doi: 10.1007/s00034-005-2403-x.
- [10] Z. Li, C. Peng, W. Tan, and L. Li, "A novel chaos-based color image encryption scheme using bit-level permutation," *Symmetry*, vol. 12, no. 9, pp. 1–17, Sep. 2020, doi: 10.3390/sym12091497.
- [11] X. Wang and N. Guan, "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation," *Optics & Laser Technology*, vol. 131, pp. 1–17, Nov. 2020, doi: 10.1016/j.optlastec.2020.106366.
- [12] J. Sun, "A 3D image encryption algorithm based on chaos and random cross diffusion," *Modern Physics Letters B*, vol. 35, no. 30, p. 2150465, Oct. 2021, doi: 10.1142/S0217984921504650.
- [13] S. Sun and Y. Guo, "A new hyperchaotic image encryption algorithm based on stochastic signals," *IEEE Access*, vol. 9, pp. 144035–144045, 2021, doi: 10.1109/ACCESS.2021.3121588.
- [14] Z. A. Abduljabbar *et al.*, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.
- [15] D. Herbadji, A. Belmeugeni, N. Derouiche, and H. Liu, "Colour image encryption scheme based on enhanced quadratic chaotic map," *IET Image Processing*, vol. 14, no. 1, pp. 40–52, Jan. 2020, doi: 10.1049/iet-ipr.2019.0123.
- [16] B. Li, X. Liao, and Y. Jiang, "A novel image encryption scheme based on logistic map and dynatomic modular curve," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8911–8938, Apr. 2018, doi: 10.1007/s11042-017-4786-7.
- [17] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Information Sciences*, vol. 520, pp. 46–62, May 2020, doi: 10.1016/j.ins.2020.02.008.
- [18] C. Li, T. Xie, Q. Liu, and G. Cheng, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1545–1551, Oct. 2014, doi: 10.1007/s11071-014-1533-8.
- [19] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019, doi: 10.1109/ACCESS.2019.2946208.
- [20] J. C. Sprott, *Chaos and time-series analysis*. Oxford: Oxford University Press, 2003.
- [21] S. Wang, Q. Peng, and B. Du, "Chaotic color image encryption based on 4D chaotic maps and DNA sequence," *Optics & Laser Technology*, vol. 148, p. 107753, Apr. 2022, doi: 10.1016/j.optlastec.2021.107753.
- [22] Z. Zhang, J. Tang, F. Zhang, H. Ni, J. Chen, and Z. Huang, "Color image encryption using 2D sine-cosine coupling map," *IEEE Access*, vol. 10, pp. 67669–67685, 2022, doi: 10.1109/ACCESS.2022.3185229.
- [23] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dynamics*, vol. 105, no. 2, pp. 1859–1876, Jul. 2021, doi: 10.1007/s11071-021-06663-1.
- [24] T. Gopalakrishnan and S. Ramakrishnan, "Image encryption using hyperchaotic map for permutation and diffusion by multiple hyper-chaotic maps," *Wireless Personal Communications*, vol. 109, no. 1, pp. 437–454, Nov. 2019, doi: 10.1007/s11277-019-06573-x.
- [25] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018, doi: 10.1016/j.sigpro.2018.06.008.
- [26] H. Ning, Y. Liu, and D. He, "Public key encryption algorithm based on Chebyshev polynomials over finite fields," in *2006 8th International Conference on Signal Processing*, 2006, pp. 1–4, doi: 10.1109/ICOSP.2006.345958.
- [27] H. M. Al-Mashhadi and I. Q. Abdaljaleel, "Color image encryption using chaotic maps, triangular scrambling, with DNA sequences," in *2017 International Conference on Current Research in Computer Science and Information Technology (ICCRIT)*, Apr. 2017, pp. 93–98, doi: 10.1109/CRCSIT.2017.7965540.
- [28] J. Hao, H. Li, H. Yan, and J. Mou, "A new fractional chaotic system and its application in image encryption with DNA mutation," *IEEE Access*, vol. 9, pp. 52364–52377, 2021, doi: 10.1109/ACCESS.2021.3069977.
- [29] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, pp. 1–11, Feb. 2020, doi: 10.1016/j.image.2019.115670.
- [30] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, Jul. 2018, doi: 10.1016/j.sigpro.2018.02.028.
- [31] J. Chen, J. Tang, F. Zhang, H. Ni, and Y. Tang, "A novel digital color image encryption algorithm based on a new 4-D hyper-chaotic system and an improved S-box," *International Journal of Innovative Computing, Information and Control*, vol. 18, no. 1, pp. 73–92, 2022, doi: 10.24507/ijicic.18.01.73.
- [32] X. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools and Applications*, vol. 77, no. 10, pp. 12349–12376, May 2018, doi: 10.1007/s11042-017-4885-5.
- [33] A. ur Rehman, X. Liao, R. Ashraf, S. Ullah, and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," *Optik*, vol. 159, pp. 348–367, Apr. 2018, doi: 10.1016/j.ijleo.2018.01.064.
- [34] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.
- [35] X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019, doi: 10.1109/ACCESS.2019.2931052.
- [36] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, Feb. 2021, doi: 10.1016/j.ins.2020.09.032.

BIOGRAPHIES OF AUTHORS

Ahmed Kamil Hasan Al-Ali    received the B.Sc. and M.Sc. degrees in electrical engineering from Al-Mustansiriyah University, Baghdad, Iraq, in 2001 and 2005, respectively, and the Ph.D. in Communication Engineering from Queensland University of Technology, Australia in 2019. He is a lecturer at the Department of Electromechanical Engineering, University of Technology. His research interests include digital signal processing, speaker recognition systems, and digital communication systems. He can be contacted at email: ahmed.k.alali@uotechnology.edu.iq.



Jafaar Mohammed Daif Alkhasraji    received his B.Sc and M.Sc degrees from Electromechanical Engineering and Laser and Optoelectronics Engineering Departments, University of Technology, Baghdad, Iraq, in 2001, and 2008, respectively, and PhD degree from Newcastle Upon Tyne, United Kingdom, in 2019. Dr. Jafaar has been a member of the syndicate of Iraqi engineers since 2002, and the IEEE community since 2016. His research interests include optical communication, wireless communication, DSP, MIMO, underwater optical wireless communication, coded and precoded OFDM communications systems, and adaptive array signal processing and estimation. He can be contacted at email: jaafar.m.dhaif@uotechnology.edu.iq.