IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 22, 2021, accepted May 8, 2021, date of publication May 17, 2021, date of current version May 25, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3081362

Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box

MUHAMMAD TANVEER[1], TARIQ SHAH[1], AMJAD REHMAN[2], (Senior Member, IEEE), ASIF ALI[1], GHAZANFAR FAROOQ SIDDIQUI[3], TANZILA SABA[2], (Senior Member, IEEE), AND USMAN TARIQ[4]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad 15320, Pakistan
[2]Artificial Intelligence and Data Analytics Laboratory, College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Department of Computer Science, Quaid-i-Azam University, Islamabad 15320, Pakistan
[4]College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Alkharj 11942, Saudi Arabia

Corresponding authors: Muhammad Tanveer (mtanveer@math.qau.edu.pk), Usman Tariq (u.tariq@psau.edu.sa), and Ghazanfar Farooq Siddiqui (ghazanfar@qau.edu.pk)

ABSTRACT The protection of digital content is increasingly becoming a significant issue for researchers and engineers. In this context, nonlinear dynamic systems play a vital role in information security through their chaotic behavior and susceptibility to initial conditions. This research presents a 3D chaotic map-based symmetric algorithm for multiple images to improve encryption efficiency and encourage secure transmission. The proposed scheme comprises the following four modules: the combination (the images are combined into a single image by merging their color channels); the permutation (using the suggested 3D chaotic map); the S-box generation; and the substitution through the AES substitution method. The proposed algorithm's encryption strength was determined through Entropy, Correlation coefficient, NPCR, and UACI analyses, which were then compared to the past techniques. Furthermore, the proposed method is assessed in terms of its computation time. Results demonstrate that it is highly efficient and secure for real-time communication.

INDEX TERMS 3*D* chaotic map, row-wise permutation, column-wise permutation, chaotic S-boxes, substitution.

I. INTRODUCTION

The protection of digital content is increasingly becoming a significant issue for researchers and engineers as millions of digital images are transmitted every second to all corners of the world. Different encryption techniques are thus applied to prevent unauthorized access to such information. These techniques provide considerable convenience of secure transmission over Internet channels.

Research in image encryption has rapidly developed in the last decade, where researchers have produced some groundbreaking work. Some of the relevant research is presented as follows: Wang *et al.* [1] used Deoxyribonucleic Acid, and Babaei *et al.* [2] used the Recursive Cellular Automata for their effective image masking techniques; a high-speed modified El Gamal encryption algorithm was proposed in [3]. In a later study [4], a controlled alternate quantum walk was used to generate random numbers for a quantum-color image masking technique. Similarly, an image masking technique was developed based on an aperture nonlinear fractional Mellin transform with extreme resistance to known-plaintext and chosen-plaintext attacks [5]. Reference [6] effectively applied the fractional domain, Arnold transforms, DWT and MSVD to design an image-masking algorithm.

It is vital to scientifically study the fundamental core of the critical problems in image encryption algorithms and then strategize new algorithms. Chaos-based encryption processes are more efficient as compared to other practical techniques. Lorenz was the first to introduce the "Butterfly effect" in 1963. He suggested the Lorenz system used in [1], [7]. Li and Yorke discovered the development from order to chaos precisely in Ref. [8]. In [9], Gladence *et al.* proposed a framework for the web-based learning and acknowledgment of signals, while Brumancia *et al.* [10] proposed a

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

suitable fuzzy-based neural model for improved decision-making. Similarly, Hamamreh *et al.* proposed a small-scale Nonorthogonal communication technique to enhance the wireless network security [11], while Zia et. al, proposed advanced Nonorthogonal multiple access security technique for the same purpose [12]. Hamamreh et. al, proposed many techniques to enhance the physical layer security [13]–[16].

Researchers have recently developed several algorithms based on neural networks [17]. Particularly, the pseudo-random number sequences are efficiently generated, employing a composite chaotic map in [17] and chaotic Hopfield neural network for the permutation and diffusion by bit XOR operation in [18]. The proposed scheme has achieved a high degree of security, but the diffusion portion is not secure enough to withstand the plaintext attacks, so the scheme's security has some question marks. The Boltzmann machine is more effective for encryption than neural networks [19]; the restricted Boltzmann device is utilized to generate the pseudo-random numbers that continuously adjust the weight matrix among the hidden and visible layers. Similarly, the ultimate weight matrix is used as a pseudo-random number matrix [17]. Finally, the XORing bit operation with the plain image accomplishes the encryption. The developed scheme has some faults like lack of permutation, which weakens the diffusion segment and has a small key space.

Modified fuzzy cellular neural networks are introduced in [20], chaotic fuzzy cellular neural networks with high sensitivity efficiently provide plaintext sensitivity and key sensitivity. The major drawbacks of this algorithm are the absence of a permutation process and the slow rate of encryption/decryption [17]. The image encryption scheme in [21] is known as the Chaotic Neural Network (CNN), having two phases (3-layer neurons). These phases are named the chaotic neuron layer and permutation neuron layer, used in the diffusion part and the permutation part of image pixel values, respectively. Lusystems, Chua, and Lorenz bring on the bias vector of the chaotic neuron layer and weight matrix, and a tent map is used as the activation function. In the permutation of the neuron layer, a cat map is utilized for scrambling the pixel position. The drawbacks of this scheme are: it is applicable on limited image types and the tent map has a low degree of nonlinearity. Further, the diffusion phase weakens the security of the overall algorithm. Similarly, some other techniques are presented in Ref. [7] and [22].

In Ref. [23], [24], Huang *et al.*, and Lidong *et al.*, proposed double-image encryption and triple-image compression encryption algorithms based on chaotic system, S-boxes, compression, and interpolation. In Ref. [25], Patro *et al.* presented a multi-color image encryption scheme through a multi-level scrambling operation. Moreover, the hash value of the image has been linked with the integrated PWLCM system to improve the security of the encryption scheme. Although Patro's scheme improves encryption efficiency to some extent, it does not consider compressing more vivid images to reduce storage space and transfer costs. There are similar deficiencies in the Ref. [26], [27]. Similarly, several researchers present chaotic multi-image encryption algorithms in Ref [28]–[32].

The encryption schemes in these articles focus on one aspect out of two (confusion & diffusion). Confusion is obtained by a substitution process, while for diffusion, chaotic maps and permutations are used. A highly secure scheme has a balance of confusion and diffusion. This article integrates confusion through Substitution-box and diffusion through a chaotic map to achieve a balanced scheme. In the proposed work, a permutation substitution encryption method is used.

i. The suggested multi-image encryption scheme is based on the 3D chaotic map.
ii. The pixels of multi-images are permuted with suggested chaotic sequences to ensure reliability and randomness.
iii. The pixels of the combined image are changed with suggested chaotic sequences after permuting them in row and column to withstand the attacks and achieve better results.
iv. The suggested 3D chaotic map is used to improve the key's sensitivity and create substantial inconsistencies in the image pixels.
v. An excessive number of parameters can increase resistance to an attack, and the amount of information leakage is reduced with increasing randomness.
vi. The superiority and the efficiency of the suggested scheme are investigated through the simulation and the comparison results.

The article is categorized as:

- Section II presents the modeling of a 3*D* chaotic map.
- The proposed scheme is outlined in section III.
- The simulation results and comparisons are explored in section IV.
- Section V concludes the article.

II. 3D CHAOTIC MAP

This section suggests a chaotic map for a more efficient multi-image encryption scheme. The suggested 3D chaotic map is defined as:

$$\begin{aligned} x_{(u+1)} &= \mu^m \cdot \sin(x_u) + y_u - \lambda^m \cdot \cos(z_u) \\ y_{(u+1)} &= \sin(x_u) \cdot \cos(y_u + x_u + \tan(z_u)) \\ z_{(u+1)} &= y_u \cdot \cos u + x_u \cdot \sin u - \psi^m \cdot \tan^{-1}(y_u) - \sigma \quad (1) \end{aligned}$$

ψ, μ, λ and σ are the control parameters, *x, y, z* are the variables and *u, m* are nonnegative integers as *m* represents the exponent.

Every chaotic system exhibits chaotic behavior for a specific interval of control parameters and initial values. The interval for control parameters for system (1) is $0 \leq \lambda, \psi \leq 2$, $0 \leq \mu, \sigma \leq 1$. Further, *x, y, z* are the obtained pseudo-random sequences, where $-8 \leq x \leq 8$, $-1 \leq y \leq 1$, $-8 \leq z \leq 8$ and $0 \leq m \leq 10$.

As an example, the chaotic behavior of the suggested map for the initial values $x_1 = 0.0005, y_1 = 0.00001, z_1 =$

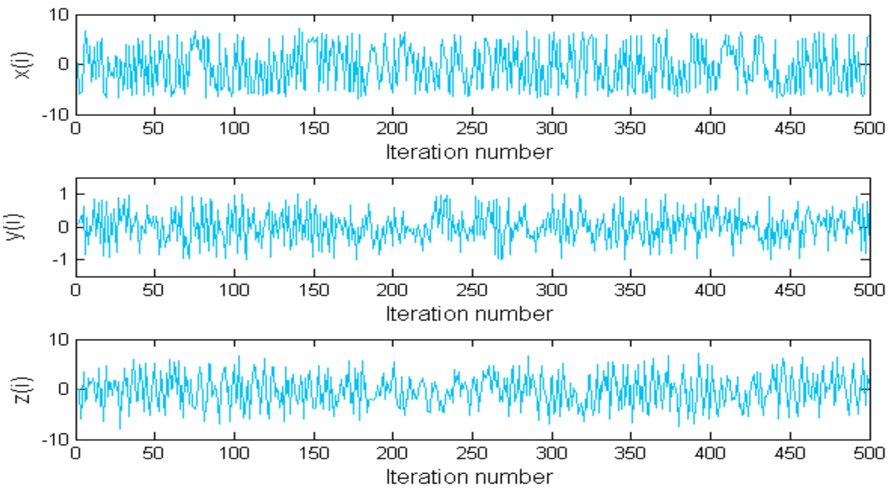


FIGURE 1. Chaotic performance of the suggested chaotic X, Y and Z sequences.

0.0038, $\psi = 15.13$, $\mu = 066$, $\lambda = 1.33332$ and $\sigma = 0.1$ is presented in Fig. 1. The non-uniform histograms of the suggested chaotic sequences are made uniform by the histogram equalization approach [33]. The histograms of the proposed sequences are shown in Fig. 2. Fig. 3 illustrates the $2D$ and $3D$ chaotic trajectories of the suggested dynamic system. The chaotic sequences and trajectories obtained by the 3D chaotic map are distributed uniformly and have complex chaotic behavior, which is suitable for image encryption.

III. PROPOSED ENCRYPTION SCHEME

The proposed multi-image encryption scheme is explored in this section. The scheme is based on the chaotic map and is described by four modules.

A. Combine images and RGB channels
B. Permutation of the combined RGB channels
C. Construction of substitution boxes
D. Substitution of permuted RGB channels

A. COMBINE IMAGES AND RGB CHANNELS

Let $I_1, I_2, I_3,$ and I_4 be the RGB images of dimension $M \times N \times 3$. Initially, the scheme merges each color component of the images I_i for $1 \leq i \leq 4$ into a single matrix. Then combine the color components to produce a single image I_m of dimension $2M \times 2N \times 3$. Once obtained, this matrix is processed through the following modules to encrypt the image I_m.

B. PERMUTATION OF RGB CHANNELS

In digital images, up to fifteen neighboring pixels are highly correlated; therefore, a well-organized pattern should destroy the pixel intra-correlation. This module permutes the pixel's position of the combined image (single image) using the map given in the Eq. (1). To mix the data of each image in a nonlinear manner, the chaos generated by the suggested nonlinear map is used in the permutation process. The mathematical representation of the permutation process is given in four cases as follows.

1) ROW-WISE PERMUTATION

a: CASE I

$$I_p(u, v) = I(u - x_u, v) \quad \text{if } u - x_u \geq 1 \text{ and } x_u = 2q \text{ for some } q \in \mathbb{Z} \tag{2}$$

b: CASE II

$$I_p(u, v) = I(u + M - x_u, v), \quad \text{if } u - x_u < 1 \text{ and } x_u = 2q \text{ for some } q \in \mathbb{Z} \tag{3}$$

c: CASE III

$$I_p(u, v) = I(u - x_u, v), \quad \text{if } u - x_u \leq M \text{ and } x_u = 2q + 1 \text{ for some } q \in \mathbb{Z} \tag{4}$$

d: CASE IV

$$I_p(u, v) = I(u + x_u - M, v) \quad \text{if } u - x_u > M \text{ and } x_u = 2q + 1 \text{ for some } q \in \mathbb{Z} \tag{5}$$

2) COLUMN-WISE PERMUTATION

a: CASE I

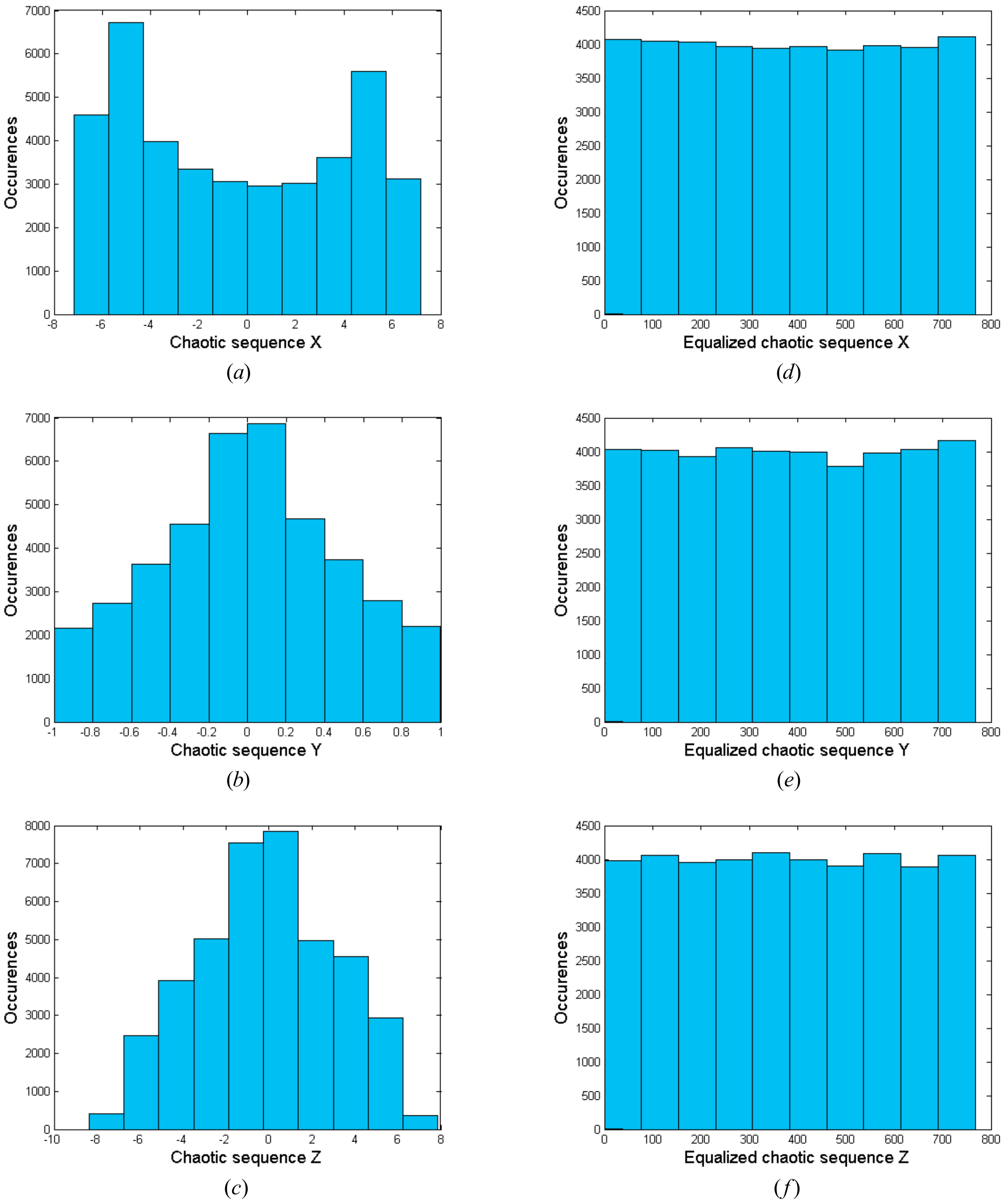
$$I_p(u, v) = I(u - x_u, v) \quad \text{if } u - x_u \geq 1 \text{ and } x_u = 2q \text{ for some } q \in \mathbb{Z} \tag{6}$$

b: CASE II

$$I_p(u, v) = I(u + M - x_u, v), \quad \text{if } u - x_u < 1 \text{ and } x_u = 2q \text{ for some } q \in \mathbb{Z} \tag{7}$$

c: CASE III

$$I_p(u, v) = I(u - x_u, v) \quad \text{if } u - x_u \leq M \text{ and } x_u = 2q + 1 \text{ for some } q \in \mathbb{Z} \tag{8}$$



(*a*)

(*d*)

(*b*)

(*e*)

(*c*)

(*f*)

FIGURE 2. **Histograms of suggested sequences 2(a-c): Histograms before equalization, 2(d-f): Histograms after equalization.**

d: CASE IV

$$I_p(u, v) = I(u + x_u - M, v)$$
$$\text{if } u - x_u > M \text{ and } x_u = 2q + 1 \text{ for some } q \in \mathbb{Z} \qquad (9)$$

$I(u, v)$ and $I_p(u, v)$ denotes the pixel values of the original and the permuted image, respectively.

All pixel values in the original image are row-wise permuted, followed by a column-wise permutation, depending on the value of the chaotic sequence. The consequent matrix is represented by I_p. In the proposed work, the column-wise permutation process is the same as the row-wise permutation. However, a different approach for the two permutations can be used to induce further complexity.

C. CONSTRUCTION OF SUBSTITUTION BOES

The substitution box is an essential part of any symmetric key cryptographic scheme. Therefore, this module generates an S-box and then uses it for the substitution. The S-box construction procedure is given as.

$$y_i'' \equiv y_i \bmod 256 \qquad (10)$$

Defined a map:

$$S : y_i'' \rightarrow \mathbf{Z}_{256}$$

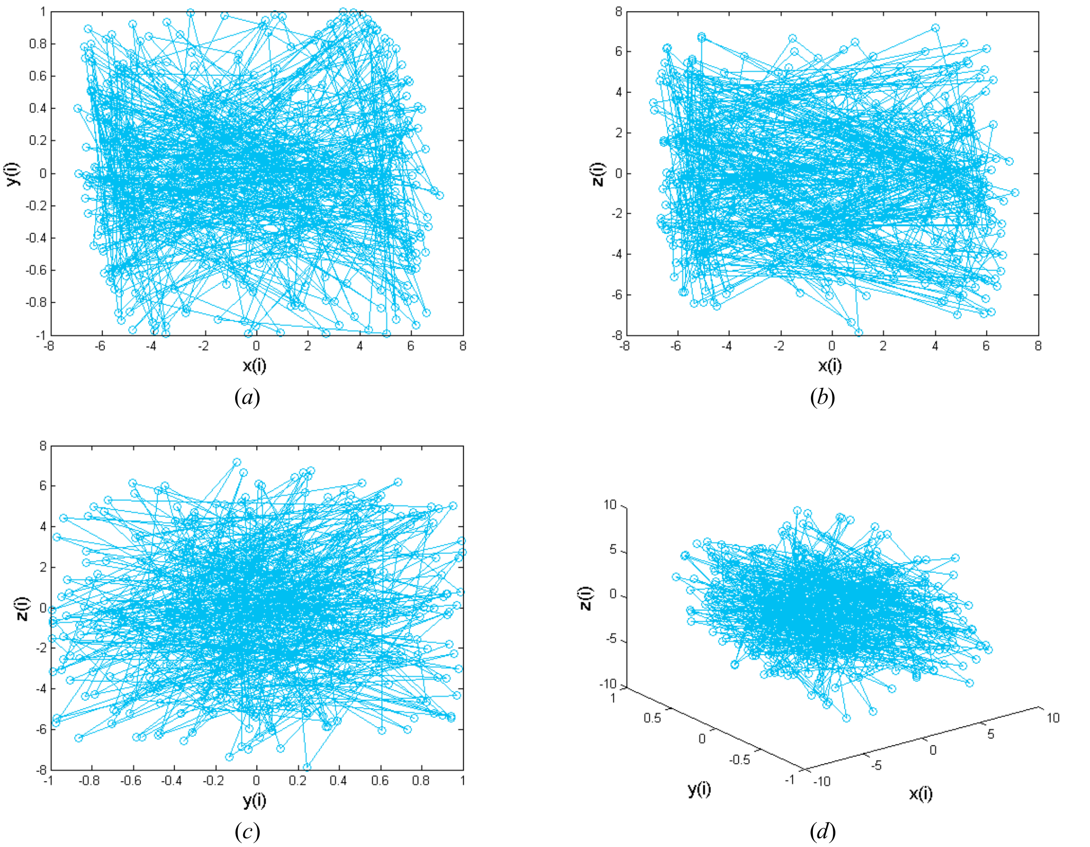


FIGURE 3. 2D and 3D chaotic trajectories of suggested chaotic map 3(a): the trajectory of (x_i, y_i); 3(b): the trajectory of (x_i, z_i); 3(c): the trajectory of (y_i, z_i); 3(d): the trajectory of (x_i, y_i, z_i).

$$S(y_i'') = \begin{cases} y_i'' & \text{if } y_i'' \neq S, \forall 1 \leq j \leq i-1 \\ 0 & \text{if } y_i'' = S, \exists 1 \leq j \leq i-1 \end{cases} \qquad (11)$$

The map S is an onto map that contains random numbers from 0 to 255. For a different value of the initial condition and the parameter, the scheme generates different S-boxes which preserve all the cryptographic properties.

D. SUBSTITUTION OF PERMUTED RGB CHANNELS

The substitution is performed through the S-boxes generated in module 3 in the last module through the AES substitution method. The resultant image is encrypted I_e.

The flowchart of the scheme, the results of the combined and individual encrypted images are demonstrated in Fig. (4-6), respectively. Fig. 5 shows that the ciphered and original images have no relationship, but later the decryption gives the original image. In Fig. 6, the original, permuted, and ciphered images of Lena, Mandrill, Peppers and Deblur are provided. Both figures demonstrate that the scheme has exceptional encryption and decryption properties.

IV. SIMULATION RESULTS AND ANALYSES

In our suggested work, standard color images of ‘‘Lena’’, ‘‘Peppers’’, ‘‘Mandrill’’, and ‘‘Deblur‘‘ have been used as test images.

The combined multi-image, its ciphered and deciphered images are provided in Fig. 5(a), 5(b), and 5(c), respectively. Furthermore, individual plain images, their permuted and ciphered images are displayed in Fig. 6$(a-d)$, 6$(e-h)$, and 6$(i-l)$, respectively. For the execution of both the encryption and decryption process, the computerized simulations are conducted in MATLAB R2013a (8.1.0.604).

A. HISTOGRAM ANALYSIS

The histogram analysis is presented to evaluate the uniform distribution of ciphered [34]. A cryptosystem has a high resistance to the statistical attacks if the probability of each gray value in the uniform histogram is the same [34].

In Fig. 7, the original, the ciphered, and their corresponding histograms of the multi-image and single images are displayed. These histograms demonstrate that the pixels of the ciphered images are more evenly spread than the original images. This aspect ensures that the proposed scheme has high resistive capability against differential, plaintext, and statistical attacks.

B. KEY SENSITIVE ANALYSIS

The key plays a vital role in testing the strength of the encryption scheme [35]. A cryptosystem has a high key sensitivity if the decryption with slightly different key outputs different images instead of plain image [36].

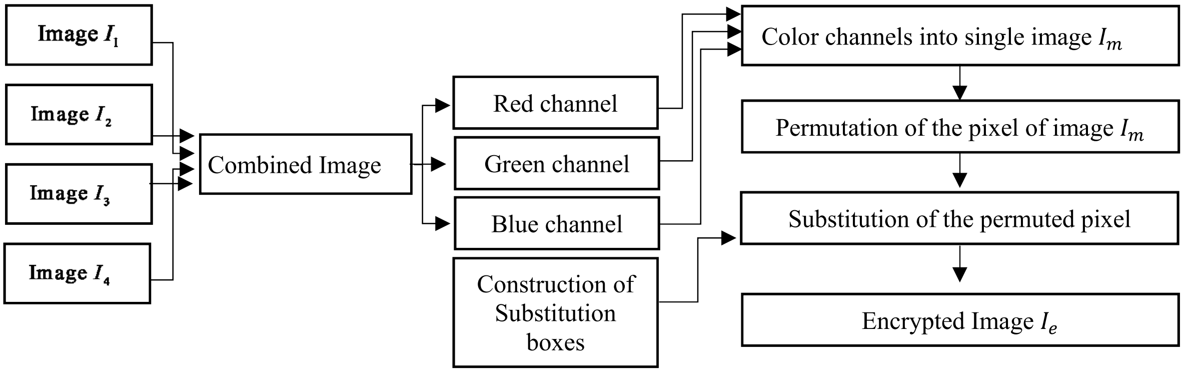


Image I_1
Image I_2
Image I_3
Image I_4
Combined Image
Red channel
Green channel
Blue channel
Construction of Substitution boxes
Color channels into single image I_m
Permutation of the pixel of image I_m
Substitution of the permuted pixel
Encrypted Image I_e

FIGURE 4. Flow chart of the encryption process.

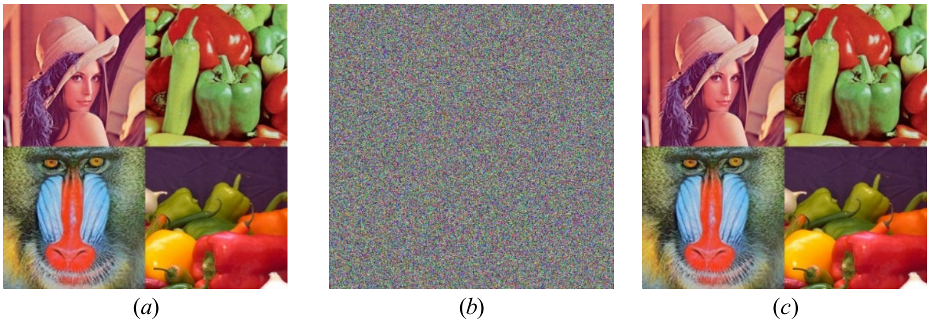


FIGURE 5. Encryption outcomes, 5(a) Plain image; 5(b) Encrypted image; 5(c) Decrypted image.

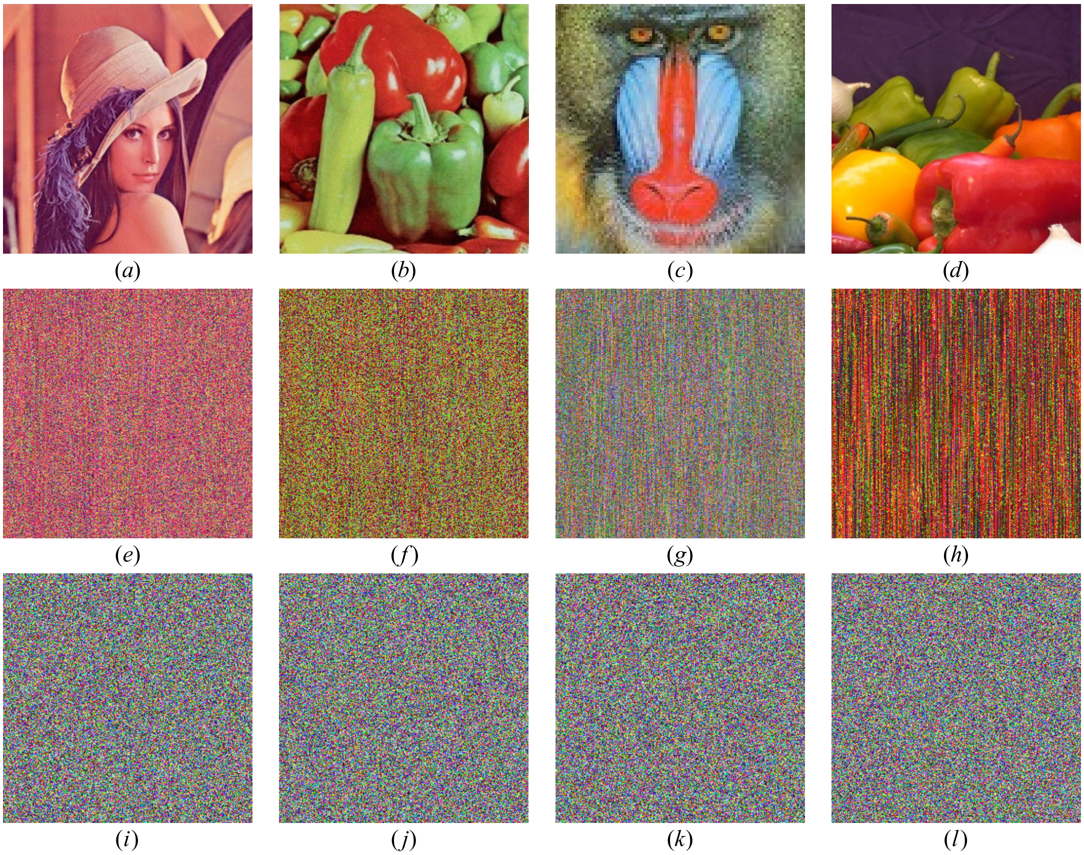
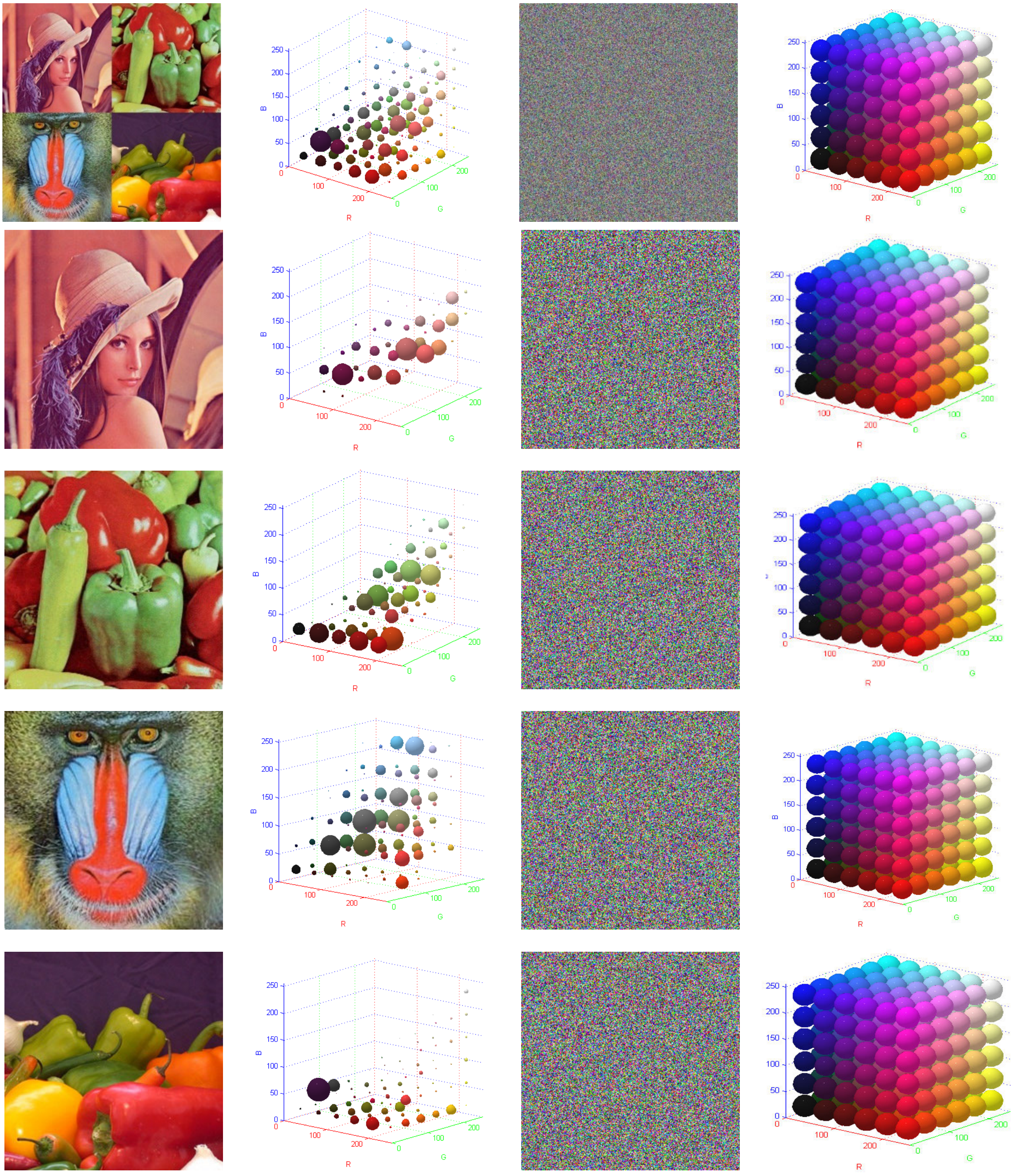


FIGURE 6. Experimental outcomes 6(a-d) Plain images; 6(e-h) permuted images; 6(i-l) encrypted images.

To appraise the key sensitivity of the suggested scheme, two keys K_1 and K_2 which are slightly different from each other are compared. The Lena test image is encrypted using K_1 and K_2. The demonstration is provided in Fig. 8. The plain



(*a*) (*b*) (*c*) (*d*)

FIGURE 7. Histogram of original and encrypted images. 7(a): plain images; 7(b): corresponding histograms; 7(c): encrypted images; 7(d) corresponding histograms.

image is given in 8(a). The encryption of plain images with K_1 and K_2 are given in 8(b) and 8(c), respectively. The difference between encrypted images is given in 8(d). During the decryption of 8(b) with key K_1, the original image is obtained, but this is not the case with key K_2, where the obtained image is shown in 8(f). Likewise, during the decryption of 8(c) with key K_1, the obtained image is shown in 8(g) which is not same as the original image, at the same time we obtain the original image with key K_2. This analysis ensures the capability of the scheme to yield different ciphered images when encryption is performed with slightly different keys.

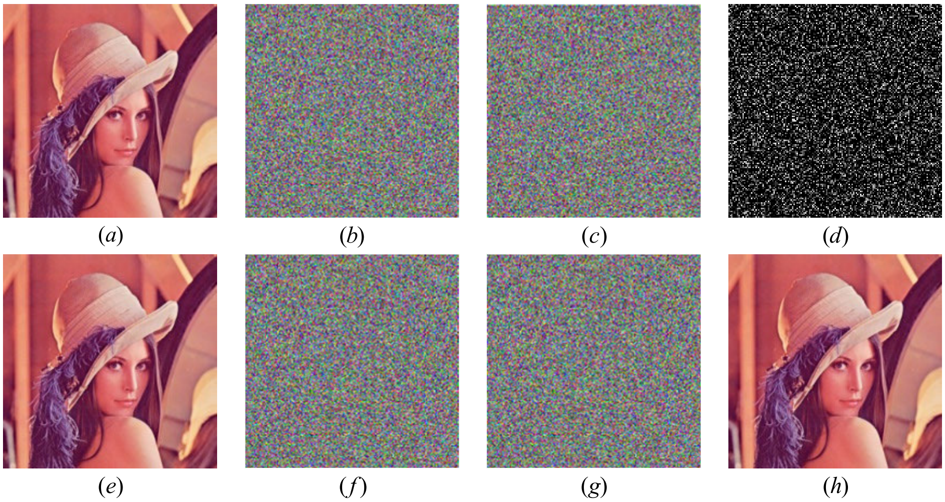


FIGURE 8. Key sensitive analysis.

TABLE 1. Information entropy analysis.

Test Image	Information entropy (Original)			Information entropy (Encrypted)		
	Red	Green	Blue	Red	Green	Blue
Combine	7.7599	7.6978	7.6571	7.9991	7.9954	7.9963
Lena	7.3277	7.6048	7.1326	7.9977	7.9945	7.9943
Peppers	7.3920	7.3920	7.1738	7.9965	7.9969	7.9932
Deblur	7.6646	7.1724	6.4954	7.9971	7.9957	7.9949
Mandrill	7.6634	7.3871	7.6646	7.9967	7.9931	7.9939

C. INFORMATION ENTROPY ANALYSIS

Entropy estimates the strength of a cryptographic scheme in terms of how much it can disorganize the encrypted image [34], [37]. It measures the degree of randomness of an encryption scheme [38]. The expression to compute the degree of randomness is given as [34].

$$H(m) = -\sum_{u=0}^{255} p(m_u) \log_2 p(m_u) \tag{12}$$

m and $p(m_u)$ are the unique random variable and probability of m_u.

A cryptosystem has a high degree of randomness if its entropy estimation is 8. The entropy analysis of the original and the ciphered image is presented in Table 1. Note that the randomness of the ciphered image is in proximity to the optimum value. Consequently, the suggested scheme can randomize the pixels to their optimum level.

D. CORRELATION ANALYSIS

It examines the strength of the encryption scheme to determine how much it can break the relationship of neighboring pixels [39]. In the plain image, the adjacent pixels are highly correlated. A good encryption scheme can break this relationship [37]. Two thousand pairs are randomly chosen to analyze adjacent correlation coefficients. The following expressions are used to calculate the correlation coefficient.

$$r_{u,v} = \frac{E((u-E(u))(v-E(v)))}{\sqrt{D(u)D(v)}}, \tag{13}$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i, \tag{14}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N} (u_i - E(u))^2, \tag{15}$$

$E(u)$ and $D(u)$ are the mathematical expectation and covariance [34].

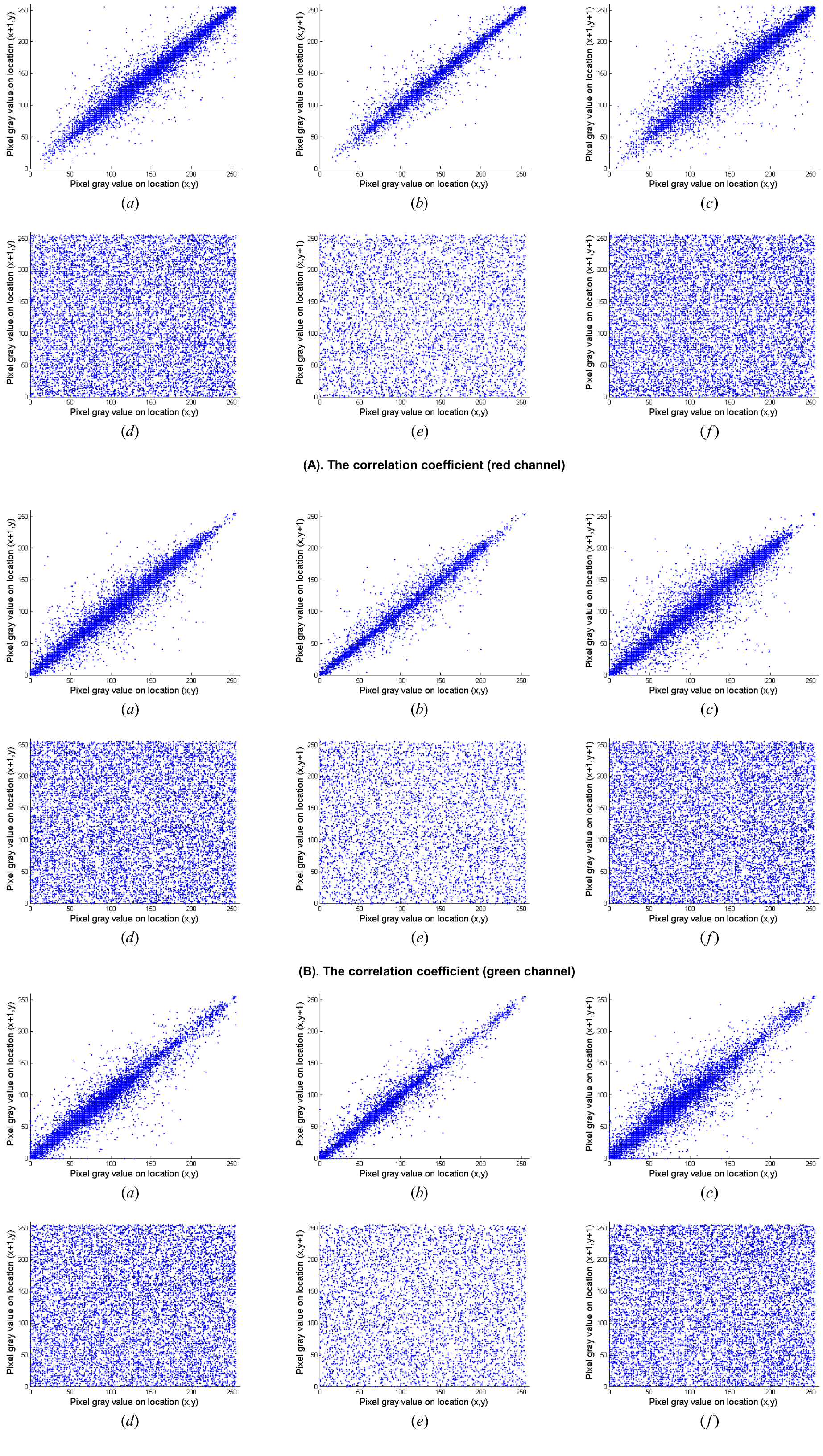
A cryptosystem has more strength if its correlation estimation is 0. The original image has a correlation close to 1 and the correlation of our test images is close to 0. This suggests that the proposed scheme is capable to break the relationship of adjacent pixels. The results of the correlation analysis of the original and the ciphered images are provided in Fig. 9(A) - 9(C), and Table 2. In Fig. 9(A) - 9(C), (a-c) and (d-f) represent the horizontal, vertical, and diagonal correlation of original and encrypted image, respectively.

E. DIFFERENTIAL ATTACKS

The association between the pixels of the plain image and the ciphered image is evaluated by the NPCR and UACI analyses [34].

A cryptosystem is secure if it is highly sensitive to minor changes in input. Suppose C_1 and C_2 are two ciphers of plain images. The following expressions are used to calculate NPCR and UACI.

$$NPCR = \frac{1}{W \times H}\left[\sum_{u,v} D(u,v)\right] \times 100\%, \tag{16}$$



(A). The correlation coefficient (red channel)

(B). The correlation coefficient (green channel)

(C). The correlation coefficient (blue channel)

FIGURE 9. **(A). The correlation coefficient (red channel). (B). The correlation coefficient (green channel). (C). The correlation coefficient (blue channel).**

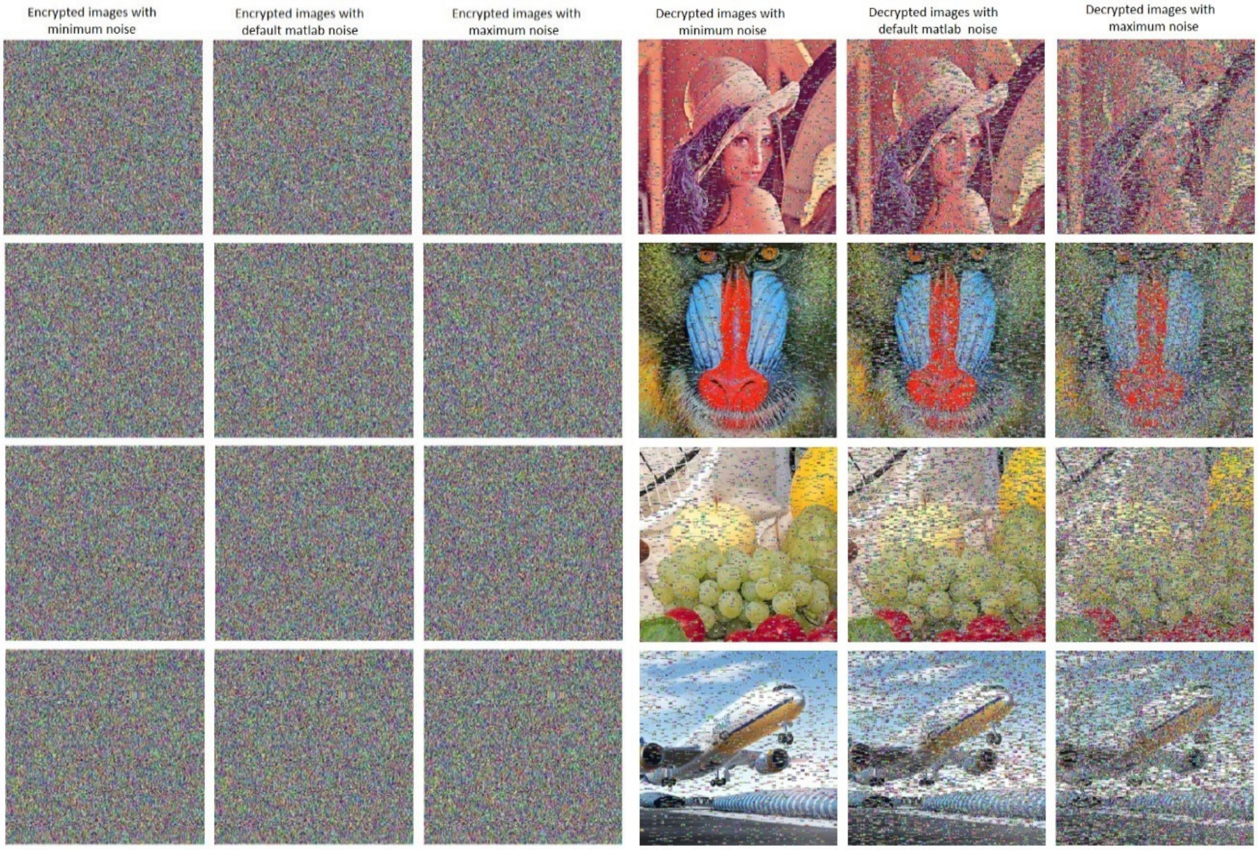

Encrypted images with minimum noise
Encrypted images with default matlab noise
Encrypted images with maximum noise
Decrypted images with minimum noise
Decrypted images with default matlab noise
Decrypted images with maximum noise

FIGURE 10. Noise analysis.

TABLE 2. Correlation analysis.

Test Image	Correlation (Original)			Correlation (Encrypted)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Combine	0.9724	0.9718	0.9386	0.0016	-0.0056	0.0015
Lena	0.9452	0.9438	0.9048	-0.00243	-0.00187	-0.00254
Peppers	0.9369	0.9272	0.9637	-0.0174	-0.0105	-0.0241
Deblur	0.9848	0.9903	0.9825	-0.0291	-0.0014	-0.0149
Mandrill	0.9419	0.9656	0.9114	0.0065	-0.0187	-0.0054

TABLE 3. NPCR and UACI results.

Schemes	NPCR			UACI		
	Blue (%)	Green (%)	Red (%)	Blue (%)	Green (%)	Red (%)
Combine	99.6063	99.6017	99.5997	33.3846	33.4102	33.2960
Lena	99.5925	99.5921	99.5917	33.0371	33.3102	33.0319
Peppers	99.6014	99.6174	99.6275	33.1504	33.0761	33.2046
Deblur	99.6032	99.6051	99.5961	33.5202	33.2466	33.2779
Mandrill	99.5809	99.5992	99.5975	33.4076	33.1655	33.2769

$$UACI = \frac{1}{W \times H}\left[\sum_{u,v}\frac{C_1(u,v) - C_2(u,v)}{255}\right] \times 100\%, \quad (17)$$

$C_1(u,v)$ is the gray pixel value of the cipher image [34].

$$D(u,v) = \begin{cases} 1 & C_1(m,n) \neq C_2(m,n) \\ 0 & otherwise \end{cases} \quad (18)$$

These analyses are evaluated, and the findings are presented in Table 3. These findings indicate the suggested scheme's high resistance to differential attacks.

F. KEYSPACE ANALYSIS

It is important to test the brute force attack to test the security strength of the cryptosystem [40]. A cryptosystem can withstand the brute force attack if its key space is

TABLE 4. Image quality measure for 256 × 256 multi-image.

Quality measure	Encrypted Image			Optimal		
	Red	Green	Blue	Red	Green	Blue
SSIM	0.0069	0.0082	0.0320	0.0077	0.0054	0.0186

TABLE 5. NIST test results.

Test		P – values Encrypted Image			Result	
		Red	Green	Blue	Random	Nonrandom
Frequency		0.49672	0.81027	0.24957	☑	
Block Frequency		0.2314	0.03474	0.79895	☑	
Rank		0.28911	0.29892	0.29781	☑	
Runs (M=10,000)		0.81517	0.96785	0.74577	☑	
Long Runs of ones		0.7126	0.7126	0.7126	☑	
Overlapping Templates		0.86598	0.82166	0.85789	☑	
No Overlapping Templates		0.99326	0.99819	0.99628	☑	
Spectral DFT		0.25474	1	0.47686	☑	
Approximate Entropy		0.052736	0.70132	0.6312	☑	
Universal		0.98108	0.99878	0.99115	☑	
Serial	p values 1	0.029565	0.19870	0.13674	☑	
Serial	p values 2	0.003765	0.03782	0.15076	☑	
Cumulative Sums Forward		0.093897	0.23879	0.10914	☑	
Cumulative Sums Reverse		1.1715	0.61785	0.91678	☑	
Random Excursions	$X = -4$	3.45E-15	0.23178	0.62765	☑	
	$X = -3$	0.59549	0.00343	0.61652	☑	
	$X = -2$	0.01279	0.5343	0.93581	☑	
	$X = -1$	0.7138	0.81799	0.93472	☑	
	$X = 1$	0.91818	0.9402	0.01759	☑	
	$X = 2$	0.97863	0.89732	0.87874	☑	
	$X = 3$	0.99435	0.034587	0.56754	☑	
	$X = 4$	0.9895	0.031562	0.63204	☑	
Random excursions variants	$X = -5$	0.13454	0.32821	0.30243	☑	
	$X = -4$	0.70664	0.28653	0.62678	☑	
	$X = -3$	1	0.19349	1	☑	
	$X = -2$	0.78392	0.17659	0.83415	☑	
	$X = -1$	0.62617	0.19947	0.89837	☑	
	$X = 1$	0.31843	0.34674	0.30262	☑	
	$X = 2$	0.5726	0.48946	0.37325	☑	
	$X = 3$	0.66354	0.74845	0.19643	☑	
	$X = 4$	0.71657	0.83143	0.05465	☑	

greater than $10^{30} \approx 2^{100}$. Assume that the precision of the computer is 10^{15}. The keys of the 3D chaotic map are $x_1, y_1, z_1, \psi, \mu, \lambda$ and σ. Thus, the key space has a total of $10^{105} \approx 2^{348}$ possibilities. It shows that the key space of the proposed scheme is enormous in its ability to withstand the brute force attack.

G. TIME EXECUTION ANALYSIS

The time required for algorithm execution is also of critical importance to test the value of a cryptosystem [41]. The proposed algorithm is tested on a machine with the following specs: Intel(R) Core (TM) i3-4010U processor @ 1.70GHz; 4.00 GB RAM; and Windows 10 Enterprise. For the execution of both the encryption and decryption process, the computerized simulations are conducted in MATLAB R2013a (8.1.0.604). The time taken to encrypt the RGB Test image is 19.922 seconds.

H. NOISE ANALYSIS

When exposed to some noise in the transmission, the behavior of the cipher scheme is of critical importance. Rarely, there is some noise in the broadcast channel. As a result,

TABLE 6. Comparison of experimental finding with some existing techniques.

Measures	Channels	Proposed	Ref. [45]	Ref. [46]	Ref. [47]	Ref. [48]	Ref. [49]	Ref. [50]	Ref. [51]
Entropy	Red	7.9984	7.9974	7.9971	7.9968	7.9798	7.9895	7.9913	7.9874
	Green	7.9987	7.9969	7.9969	7.9965	7.9795	7.9894	7.9914	7.9872
	Blue	7.9989	7.9979	7.9962	7.9965	7.9797	7.9894	7.9916	7.9866
NPCR	Red	99.6163	99.623	99.5864	-	99.5925	99.6369	99.6113	99.5990
	Green	99.6170	99.606	99.2172	-	99.5921	99.6174	99.6060	99.5777
	Blue	99.6259	99.652	99.8474	-	99.5927	99.6054	99.6052	99.5990
UACI	Red	33.6476	33.245	33.4834	-	33.5039	33.8547	33.4280	33.4808
	Green	33.6116	33.362	33.6399	-	33.5112	33.7619	33.4966	33.1617
	Blue	33.6068	33.521	33.2689	-	33.5037	33.6046	33.3779	33.6066
Correlation	Horizontal	-0.00243	-0.00009	0.0054	-0.0065	0.0037	0.0023	-0.0080	-0.0580
	Vertical	-0.00187	-0.0011	0.0062	0.0033	0.0030	-0.0059	0.0098	-0.0024
	Diagonal	-0.00254	-0.0010	0.0017	-0.0037	-0.0029	0.0029	-0.0058	-0.0170

the encrypted image gets affected severely, and cryptosystem failed to recover the image [42]. Hence, a cryptosystem is strong if it has image retrieval property even if there is noise. Here, the effectiveness of the proposed scheme is analyzed.

Consider the analysis of fat-tail distribution, also known as salt and pepper noise [42]. There are bright pixels in the dark and dark pixels in the bright in this type of noise. In Fig. 10, encrypted and decrypted images of Lena, Baboon, Fruits and Airplane with increment in noise are given.

It is evident that the proposed scheme can recover the original image in each case of noise.

I. STRUCTURAL SIMILARITY (SSIM)

To evaluated the resemblance among two images, SSIM is performed [43]. This index is assessed on various windows of an image. The following expression is used to measure SSIM index between windows X and Y of communal size $N \times N$:

$$SSIM(X, Y) = \frac{(2\mu_X \mu_Y + c_1)(2\sigma_X \sigma_Y + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)} \tag{19}$$

$\mu_X, \mu_Y, \sigma_X^2, \sigma_Y^2, \sigma_{XY}$ are the average, variance and covariance of X and Y, respectively. Further, $c_1 = (k_1 L)^2$ and $c_1 = (k_2 L)^2$ are the variables to stabilize the division with the weak denominator, L is the dynamic range of the pixel values, $k_1 = 0.01$ and $k_2 = 0.03$ by default. The results are shown in Table 4.

J. RANDOMNESS TEST

The security level of a cryptosystem can be determined by finding its distribution, complexity, period, and output data. A cryptosystem is safe if the data is evenly distributed, so it exhibits high complexity and durability [44]. In this paper, NIST SP 800–22 [33] test is performed on a multi-image. There are also some subcategories in this test. Test results show that the encrypted test image using the proposed scheme passes all the security threats. The NIST test results are presented in Table 5.

K. COMPARISONS

The experimental findings of Entropy, Correlation coefficient, NPCR, and UACI of the suggested scheme are compared with some existing schemes in Table 6. Note that the entropy of the ciphered image is too close to the optimum value. Consequently, the suggested scheme is considerably more secure and has more strength. The results of NPCR and UACI of the ciphered image are 99.61% and 33.40%, respectively. These results indicate that the suggested scheme has a high resistance to differential attacks. The correlation coefficient values are very close to the optimal value.

This indicates that the suggested scheme is better than the techniques shown in comparison. Hence it is a highly secure.

V. CONCLUSION

This work proposes an efficient color image encryption scheme based on the construction of a 3D chaotic map. The suggested scheme induces confusion and diffusion in the image through four modules: combining plain images; row and column permutation; S-box construction; and S-box substitution of permuted pixels. The proposed scheme's encryption strength was determined through Entropy, Correlation coefficient, NPCR, and UACI analyses, which were then compared to the past techniques. Furthermore, the proposed scheme is assessed in terms of its computation time.

Experimental findings and security analysis indicate that the proposed scheme has a good encryption effect, high key sensitivity, high pixel randomization, and weak correlation of adjacent pixels. Furthermore, it opposes common statistical and differential attacks. A comparison with current work shows that the proposed algorithm is more secure and suitable for real-time communication.

ACKNOWLEDGMENT

The authors want to express their thanks to Artificial Intelligence and Data Analytics (AIDA) Lab (Prince Sultan University, Saudi Arabia) for their kind support for this research. They also appreciate the constructive comments of reviewers.

REFERENCES

[1] B. Wang, B. F. Zhang, and X. W. Liu, "An image encryption approach on the basis of a time delay chaotic system," *Optik*, vol. 225, Jan. 2021, Art. no. 165737, doi: 10.1016/j.ijleo.2020.165737.

[2] A. Babaei, H. Motameni, and R. Enayatifar, "A new permutation-diffusion-based image encryption technique using cellular automata and DNA sequence," *Optik*, vol. 203, Feb. 2020, Art. no. 164000, doi: 10.1016/j.ijleo.2019.164000.

[3] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017, doi: 10.1016/j.ijleo.2017.08.028.

[4] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption," *Phys. A, Stat. Mech. Appl.*, vol. 547, Jun. 2020, Art. no. 123869, doi: 10.1016/j.physa.2019.123869.

[5] M. Wang, Y. Pousset, P. Carré, C. Perrine, N. Zhou, and J. Wu, "Optical image encryption scheme based on apertured fractional Mellin transform," *Opt. Laser Technol.*, vol. 124, Apr. 2020, Art. no. 106001, doi: 10.1016/j.optlastec.2019.106001.

[6] A. Vaish and M. Kumar, "Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain," *Optik*, vol. 145, pp. 273–283, Sep. 2017, doi: 10.1016/j.ijleo.2017.07.041.

[7] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, Dec. 2019, doi: 10.1109/access.2018.2890116.

[8] T.-Y. Li and J. A. Yorke, "Period three implies chaos," *Amer. Math. Monthly*, vol. 82, no. 10, p. 985, Dec. 1975, doi: 10.2307/2318254.

[9] L. M. Gladence, C. K. Vakula, M. P. Selvan, and T. Y. S. Samhita, "A research on application of human-robot interaction using artifical intelligence," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 9, pp. 784–787, 2019, doi: 10.35940/ijitee.I1162.0789S219.

[10] E. Brumancia, S. J. Samuel, L. M. Gladence, and K. Rathan, "Hybrid data fusion model for restricted information using Dempster–Shafer and adaptive neuro-fuzzy inference (DSANFI) system," *Soft Comput.*, vol. 23, no. 8, pp. 2637–2644, Apr. 2019, doi: 10.1007/s00500-018-03734-1.

[11] J. P. Lemayian and J. M. Hamamreh, "A novel small-scale nonorthogonal communication technique using auxiliary signal superposition with enhanced security for future wireless networks," *RS Open J. Innov. Commun. Technol.*, vol. 1, no. 2, 2020, doi: 10.46470/03d8ffbd.86b0d106.

[12] M. F. Zia and J. M. Hamamreh, "An advanced non-orthogonal multiple access security technique for future wireless communication networks," *RS Open J. Innov. Commun. Technol.*, vol. 1, no. 2, 2020, doi: 10.46470/03d8ffbd.19888ce7.

[13] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5, doi: 10.1109/PIMRC.2017.8292335.

[14] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017, doi: 10.1016/j.phycom.2017.08.011.

[15] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6, doi: 10.1109/WCNC.2016.7564990.

[16] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Sep. 2018, doi: 10.1109/TWC.2018.2855163.

[17] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over blockchain," *Opt. Laser Technol.*, vol. 135, Mar. 2021, Art. no. 106610, doi: 10.1016/j.optlastec.2020.106610.

[18] X.-Y. Wang and Z.-M. Li, "A color image encryption algorithm based on hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, pp. 107–118, Apr. 2019, doi: 10.1016/j.optlaseng.2018.11.010.

[19] F. Hu, X. Xu, T. Peng, C. Pu, and L. Li, "A fast pseudo-stochastic sequential cipher generator based on RBMs," *Neural Comput. Appl.*, vol. 30, no. 4, pp. 1277–1287, Aug. 2018, doi: 10.1007/s00521-016-2753-2.

[20] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, and P. Raveendran, "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Process.*, vol. 140, pp. 87–96, Nov. 2017, doi: 10.1016/j.sigpro.2017.05.002.

[21] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, Jun. 2012, doi: 10.1016/j.engappai.2012.01.007.

[22] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *Int. J. Bifurcation Chaos*, vol. 28, no. 4, Apr. 2018, Art. no. 1850047, doi: 10.1142/S0218127418500475.

[23] W. Huang, D. Jiang, Y. An, L. Liu, and X. Wang, "A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing," *IEEE Access*, vol. 9, pp. 41704–41716, 2021, doi: 10.1109/ACCESS.2021.3065453.

[24] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, "A dynamic triple-image encryption scheme based on chaos, S-box and image compressing," *IEEE Access*, vol. 8, pp. 210382–210399, 2020, doi: 10.1109/ACCESS.2020.3039891.

[25] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102470, doi: 10.1016/j.jisa.2020.102470.

[26] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools Appl.*, vol. 79, nos. 19–20, pp. 12959–12994, May 2020, doi: 10.1007/s11042-019-08470-8.

[27] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Comput. Electr. Eng.*, vol. 62, pp. 401–413, Aug. 2017, doi: 10.1016/j.compeleceng.2016.12.025.

[28] W. Yu, Y. Liu, L. Gong, M. Tian, and L. Tu, "Double-image encryption based on spatiotemporal chaos and DNA operations," *Multimedia Tools Appl.*, vol. 78, no. 14, pp. 20037–20064, Jul. 2019, doi: 10.1007/s11042-018-7110-2.

[29] N. Zhou, H. Jiang, L. Gong, and X. Xie, "Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging," *Opt. Lasers Eng.*, vol. 110, pp. 72–79, Nov. 2018, doi: 10.1016/j.optlaseng.2018.05.014.

[30] X. Yang, H. Wu, Y. Yin, X. Meng, and X. Peng, "Multiple-image encryption base on compressed coded aperture imaging," *Opt. Lasers Eng.*, vol. 127, Apr. 2020, Art. no. 105976, doi: 10.1016/j.optlaseng.2019.105976.

[31] X. Li, X. Meng, X. Yang, Y. Yin, Y. Wang, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," *IEEE Photon. J.*, vol. 8, no. 4, pp. 1–11, Aug. 2016, doi: 10.1109/JPHOT.2016.2591441.

[32] Z. Gan, X. Chai, M. Zhang, and Y. Lu, "A double color image encryption scheme based on three-dimensional Brownian motion," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 27919–27953, Nov. 2018, doi: 10.1007/s11042-018-5974-9.

[33] P. E. Trahanias and A. N. Venetsanopoulos, "Color image enhancement through 3-D histogram equalization," in *Proc. IAPR Int. Conf. Pattern Recognit.*, vol. 3, 1992, pp. 545–548, doi: 10.1109/ICPR.1992.202045.

[34] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocessors Microsyst.*, vol. 65, pp. 1–6, Mar. 2019, doi: 10.1016/j.micpro.2018.12.003.

[35] S. M. Pan, R. H. Wen, Z. H. Zhou, and N. R. Zhou, "Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform," *Multimedia Tools Appl.*, vol. 76, no. 2, pp. 2933–2953, Jan. 2017, doi: 10.1007/s11042-015-3209-x.

[36] D. S. Malik and T. Shah, "Color multiple image encryption scheme based on 3D-chaotic maps," *Math. Comput. Simul.*, vol. 178, pp. 646–666, Dec. 2020, doi: 10.1016/j.matcom.2020.07.007.

[37] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyberjournals*, vol. 1, no. 2, pp. 31–38, 2011. [Online]. Available: http://www.cyberjournals.com/Papers/Apr2011/05.pdf

[38] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on a peter de jong chaotic map and a RC4 stream cipher," *3D Res.*, vol. 6, no. 3, pp. 1–5, Sep. 2015, doi: 10.1007/s13319-015-0062-7.

[39] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, "IEVCA: An efficient image encryption technique for IoT applications using 2-D von-Neumann cellular automata," *Multimedia Tools Appl.*, vol. 80, Oct. 2020, doi: 10.1007/s11042-020-09880-9.

[40] H. Yang, K.-W. Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 11, pp. 3507–3517, Nov. 2010, doi: 10.1016/j.cnsns.2010.01.004.

[41] L. Liu, D. Jiang, T. An, and Y. Guan, "A plaintext-related dynamical image encryption algorithm based on permutation-combination-diffusion architecture," *IEEE Access*, vol. 8, pp. 62785–62799, 2020, doi: 10.1109/ACCESS.2020.2983716.

[42] T. U. Haq and T. Shah, "12×12 S-box design and its application to RGB image encryption," *Optik*, vol. 217, Sep. 2020, Art. no. 164922, doi: 10.1016/j.ijleo.2020.164922.

[43] T. Shah, T. U. Haq, and G. Farooq, "Improved SERPENT algorithm: Design to RGB image encryption implementation," *IEEE Access*, vol. 8, pp. 52609–52621, 2020, doi: 10.1109/ACCESS.2020.2978083.

[44] F. Pareschi, R. Rovatti, and G. Setti, "On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 491–505, Apr. 2012, doi: 10.1109/TIFS.2012.2185227.

[45] A. Girdhar and V. Kumar, "A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, Oct. 2018, doi: 10.1007/s11042-018-5902-z.

[46] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, Feb. 2012, doi: 10.1016/j.jss.2011.08.017.

[47] Q. Zhang and X. Wei, "RGB color image encryption method based on Lorenz chaotic system and DNA computation," *IETE Tech. Rev., Inst. Electron. Telecommun. Eng. India*, vol. 30, no. 5, pp. 404–409, 2013, doi: 10.4103/0256-4602.123123

[48] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Jan. 2018, doi: 10.1007/s11071-017-3874-6.

[49] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern., Syst.*, pp. 1–12, Aug. 2019, doi: 10.1109/TSMC.2019.2932616.

[50] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *J. Electron. Imag.*, vol. 21, no. 1, 2012, doi: 10.1117/1.JEI.21.1.013014.

[51] L. Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3653–3659, Oct. 2014, doi: 10.1016/j.cnsns.2014.03.016.

MUHAMMAD TANVEER graduated from the University of Gujrat, in 2013. He received the Master of Philosophy degree in mathematics from the Department of Mathematics, Quaid-Azam University, in 2015, where he is currently pursuing the Ph.D. degree. His research interests include groups, rings, image encryption using substitution boxes and chaotic maps, data compression, and watermarking.

TARIQ SHAH received the Ph.D. degree in mathematics (commutative algebra) from the University of Bucharest, Romania, in 2000. He is currently a Professor with the Department of Mathematics. He is also the pioneer of introducing the field of cryptography in the mathematics department. He has published many articles in the field of finite fields and cryptography.

AMJAD REHMAN (Senior Member, IEEE) received the Ph.D. degree from the Faculty of Computing, University of Technology, Malaysia, in 2010, with a focus on forensic document analysis and security. He is currently a Senior Researcher with the AIDA Laboratory, Prince Sultan University, Riyadh, Saudi Arabia. He has more than 100 publications in the field of data mining, health informatics, and sample identification.

ASIF ALI is currently serving as an Associate Professor with the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include finite group theory, finite loop theory, solutions of highly nonlinear differential equations, and artificial intelligence.

GHAZANFAR FAROOQ SIDDIQUI received the Ph.D. degree in computer science from Vrije University Amsterdam, The Netherlands, in 2010. He is currently an Assistant Professor with the Department of Computer Science, Quaid-i-Azam University, Islamabad. Prior to that, he was a Research Scholar with Vrije University Amsterdam. He is also a reviewer of several peer-reviewed conferences and journals. He has published numerous research articles in prestigious conferences and journals.

TANZILA SABA (Senior Member, IEEE) received the Ph.D. degree in document information security and management from the Faculty of Computing, Universiti Technologi Malaysia (UTM), Malaysia, in 2012. She is currently an Associate Professor and the Associate President of the Department of Information Systems, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. With an H-index of 45, she has more than 200 publications with more than 5000 citations. Most of her publications are in biomedical research published in the ISI/SCIE index.

USMAN TARIQ received the Ph.D. degree in information and communication technology in computer science from Ajou University, South Korea. He is currently an Associate Professor with the College of Computer Engineering and Science, Prince Sattam Bin Abdulaziz University. He is also a skilled Research Engineer. He has a strong background in ad hoc networks and network communications. He is also experienced in managing and developing projects from conception to completion. He has worked in large international scale and long-term projects with multinational organizations.