




## Research Article

# A New Multistage Encryption Scheme Using Linear Feedback Register and Chaos-Based Quantum Map

Adel R. Alharbi,<sup>1</sup> Jawad Ahmad ,<sup>2</sup> Arshad,<sup>3</sup> Sajjad Shaukat Jamal ,<sup>4</sup> Fawad Masood,<sup>2,5</sup> Yazeed Yasin Ghadi ,<sup>6</sup> Nikolaos Pitropakis,<sup>2</sup> and William J Buchanan<sup>2</sup>

<sup>1</sup>College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

<sup>2</sup>School of Computing, Edinburgh Napier University, Edinburgh EH105DT, UK

<sup>3</sup>Institute for Energy and Environment, University of Strathclyde, Glasgow G11XQ, UK

<sup>4</sup>Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia

<sup>5</sup>College of Information Engineering, Yangzhou University, Yangzhou 225009, China

<sup>6</sup>Department of Computer Science and Software Engineering, Al Ain University, Abu Dhabi 122612, UAE

Correspondence should be addressed to Jawad Ahmad; [j.ahmad@napier.ac.uk](mailto:j.ahmad@napier.ac.uk)

Received 20 December 2021; Revised 10 February 2022; Accepted 2 March 2022; Published 18 April 2022

Academic Editor: Atila Bueno

Copyright © 2022 Adel R. Alharbi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the increasing volume of data transmission through insecure communication channels, big data security has become one of the important concerns in the cybersecurity domain. To address these concerns and keep data safe, a robust privacy-preserving cryptosystem is necessary. Such a solution relies on chaos encryption algorithms over standard cryptographic methods that possess multistage encryption levels, including high speed, high security, low compute overheads, and procedural power, among other characteristics. In this work, a secure image encryption scheme is proposed using linear feedback shift register (LFSR) and chaos-based quantum chaotic map. The focus of the scheme is mainly dependent on the secret keys from the input of the algorithm. The threat landscape, the statistical test analysis, along critical comparisons with other schemes indicate that the presented algorithm is significantly secure and is resistant to a wide range of different attacks such as differential and statistical attacks. The proposed method has sufficiently higher sensitivity and security when compared to existing encryption algorithms. Several security parameters validated the security of proposed work such as correlation coefficient analyses among the neighboring pixels, entropy, the number of pixels change rate (NPCR), unified average change intensity (UACI), mean square error (MSE), brute force, key sensitivity, and peak signal to noise ratio (PSNR) analyses. The randomness of the ciphers produced by the proposed technique is also passed through NIST-800-22. The results of NIST indicate that the ciphers are highly random and do not produce any type of periodicity or pattern.

## 1. Introduction

With the fast progression of data technology, a high volume of multimedia data, comprising digital images, video, and audio, is produced and distributed across various networks. Multimedia data, particularly digital images, is one of the most extensively used data formats in modern times. Since digital images contain information that can be sensitive at times, unauthorized access to a secret image can result in serious information security incidents. As a result, it is

critical to add a security layer to protect sensitive digital images. Researchers in this area have recently established numerous methodologies to securely communicate digital images, such as information hiding, data encryption, steganography, and digital watermarking. Contents in an image can be protected via image encryption algorithms. An image data encryption algorithm converts meaningful information into cipher data that is unrecognizable, thus preventing the potential intruders from extracting the original information. The original data can be fully retrieved by using the proper

key. The sensitive data cannot be retrieved by using the wrong key. Among all image encryption techniques, chaos theory is the most extensively utilized and operational technique that provides security to the data without introducing considerable overheads. This is because chaos theory shares many properties with image encryption principles [1–3].

On the other hand, chaos deprivation occurs due to precision limitations when a chaotic system is employed in a digital stage. As a result, image encryption methodologies that rely solely on chaotic schemes have numerous security flaws. Combining chaotic systems with other techniques is one effective way to solve this problem. Furthermore, several image encryption procedures based on other methodologies, such as frequency domain transformation and compressive sensing, have been suggested in the literature [2, 3].

Encrypted multimedia information such as chaos-based image security plays an essential role in the upcoming quantum computers era. With the introduction of quantum systems, concerns regarding chaos-based classical systems have drawn the attention of the cyber security community. As time passes, the classical chaos-based dynamical system becomes quantized; thus, researchers need to study the combined effect of quantum and chaotic systems. The quantum chaotic map with the bifurcation explanation was initially proposed in [4]. After that, the quantized baker's transformation was studied in [5]. The structure of the trace formula for quantum maps on a compact phase space was analyzed in [6]. Many other aspects of quantum chaos were discussed in [7–10]. The new version of the study is known as the quantum version of the classical chaotic system. The innovative quantized version of the chaos-based system using chaotic quantum system possesses better properties and provides deep insight into the nature of quantum chaos. The sensitive dependence of chaotic systems gives rise to chaos for some specific initial conditions. The new map, the quantized version (chaotic quantum map), is based on canonical transformation; however, there is no proper technique for quantizing the classical map. Many cryptographers and researchers are working on using quantum maps for image encryption in the context of quantum chaos combination.

Numerous image data encryption technique has been examined and concluded that symmetric cipher-based encryption systems require limited options and have larger bandwidth, making them appropriate for multimedia data security. Chai et al. proposed an image encryption technique based on DNA encryption and chaos [11]. Praveen et al. developed a new cryptosystem for medical image Trans receiving based on the chaos [12]. Kadir et al. utilized the concept of a hyperchaotic system of 6<sup>th</sup> order CNN and skew tent map for color image encryption [13]. Masood et al. employed the combination of chaos and DNA genetic encoding for the construction of a secure encryption scheme [14]. Fawad et al. offered a secure medical encryption algorithm based on Brownian motion, Henon chaotic map, and Chen's chaotic system with elevated security [15]. Shah et al. proposed a privacy-preserving mechanism using Dynamic Newton Leibnik and Modified logistic maps [16]. Butt

et al. applied the combination of Lucas series and Pseudo Quantum map to offer a digital image confidentiality scheme [17]. Private key ciphers are further categorized into two types: stream ciphers and block ciphers. Numerous existing block and stream ciphers produce high randomness that might be resistant to different classical attacks. However, it has been discovered that stream ciphers are slow as they encrypt one bit or one byte at a time. The stream cipher's basic operation is to yield a high-quality long pseudorandom keystream, which is then used to encode the image data. The output from several Linear Feedback Shift Register (LFSRs) can be fed into an appropriate nonlinear Boolean function to create a stream cipher. Furthermore, the utilization of bit-positioned operations in the LFSR-based algorithm, this image encryption has higher bandwidth. Because of its high throughput and low computational resource requirements, arbitrary number initiation may be a promising method for data encryption. Moreover, current workstations support the word process, and the price of creating a one bit is the equivalent as that of producing a  $w$ -bit word, where  $w$  is the machine processor's word size [18, 19]. The block size of a processor can range from 16 to 64 bits. The current review encourages us to use word-LFSR based on nonlinear functions for data encryption. Many encryption schemes based on the quantum chaotic map along with some other structures have been proposed in the literature [20–22]. But the key generation procedures in the recent quantum-based chaotic structures are independent of the plaintext which makes it vulnerable against the differential and classical attacks. Therefore, our proposed encryption structure includes the key generation based on plaintext and changes concerning the change in the input.

In this work, the combination of LFSR and quantum chaotic map has been utilized to offer an efficient image encryption approach. The suggested system is completely key-dependent. The input of the algorithm generates the initial seeds to LFSR and quantum chaotic map. The proposed encryption technique comprises confusion-diffusion architecture. Some cryptographic analysis ensures the security of the offered system. The simulation results of performance analysis indicate that the suggested encryption technique yields ciphers with high randomness and low correlation. Therefore, the proposed encryption structure is robust and secure for data transmission. The contributions of this work can be summarized as follows:

- (i) A novel multistage encryption scheme using a linear feedback register and a chaos-based quantum map is proposed
- (ii) Security of the proposed methodology against known attacks is extensively analyzed
- (iii) A comparison of the proposed methodology against competing approaches found in the literature is conducted

This manuscript is structured as follows: Section 2 offers basic concepts about cryptosystem; Structure of offered approach is defined in Section 3; In Section 4, security analyses are performed; Section 5 presents comparative

analysis; Finally, Section 6 concludes our work while giving some pointers for future work.

## 2. Some Basic Concepts

**2.1. Linear Feedback Shift Register.** LFSR is based on a logic circuit that works in a sequential order used in digital circuits to store digital data. It is built up in a linear form with inputs/outputs coupled. The process of data starts once the circuit is triggered. The input bit of LFSR yields a linear function of two or further of its preceding states, also known as taps. An LFSR of size  $n$  is made up of  $n$  stages as,  $0, 1, \dots, n-1$ , each of which may store one bit, and a clock that controls data interchange. The shift register would be initialized with a vector containing elements  $p_0, \dots, p_{n-1}$ . The following operations are carried out at time  $i$ .

- (i) The output includes  $p_i$  (the content of stage 0)
- (ii) The data of stage  $i$  is relocated to phase  $i-1$ , for  $1 \leq i \leq n-1$
- (iii) The new data (the feedback bit) of stage  $n-1$  is acquired by XORing a subsection of the  $n$  stages' data

An LFSR's initial input is referred to as a seed. Because any register can only have a restricted number of taps, it must ultimately become periodic. An LFSR with a carefully designed feedback function and seed, on the other hand, can generate a structure of bits that seems random (and has strong statistical features) and has a long period. Pseudo-random numbers, rapid digital counters, pseudo-noise sequences, cryptography, whitening sequences, and other applications can all benefit from LFSRs, which can be employed in hardware and software. There are many alternative setups such as Figure 1 illustrates a simple setup that starts with an input of all 1's and is very simple to employ in hardware and software. An LFSR of this category will never encompass only 0's and will stop if a binary string containing only 0's is input into it. Only certain tap combinations (i.e., the nonzero coefficients  $c_i$  described below) will result in a maximum sequence with a period of  $2^n - 1$  series. If the initial (left) 4 bits are given to the LFSR, the subsequent sequence will be generated:

1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1.

If the content of the phase  $p_i$  is  $p_i$ ,  $0 \leq i \leq m-1$ , then  $[p_{m-1}, \dots, p_1, p_0]$  is known as the initial state of the LFSR. From the description of an LFSR, the yielded sequence  $p_0, p_1, \dots$  will satisfy the subsequent recursion

$$p_j = \sum_{i=1}^m c_i p_{j-i}, \quad j \geq m. \quad (1)$$

The polynomial  $C(x) = 1 + c_1x + \dots + c_mx^m$  is the feedback (or connection) polynomial of the sequence  $\{c_j\}_j = \{p_j: j = 0, 1, \dots\}$ . The LFSR is nonsingular if  $c_m = 0$ , that is, the degree of its feedback polynomial is  $m$ .

As the powers in the linear feedback function are 16, 14, 13, 11, the bits at these situations are XORed. The bits are

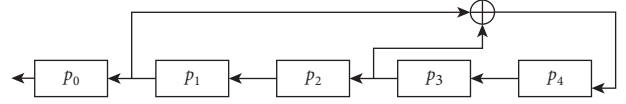


FIGURE 1: LFSR with five stages  $p_i$ , and feedback bit  $p_4 = p_1 \oplus p_3$ .

shifted by 1, and then the XORed value is maintained as the first bit. The pseudoalgorithm explaining the general scenario of the linear feedback shift register is presented in Algorithm 1.

**2.2. Quantum Chaotic Map.** This section presents a high-level summary of the quantum logistic map. The logistic map is discussed in [23] when the dissipation parameter is increased. Goggin et al., [24] developed a chaos-based quantum map that was dissipative by attaching a harmonic oscillator (quantum kicked) and observing the resulting dissipation. They write  $p = p + \delta p$  to explore the properties of quantum corrections, where  $\delta p$  signifies a quantum fluctuation about  $p$  [24], and  $p$  represents a quantum correction. The following differential equations govern this map with the lower order quantum corrections:

$$\begin{cases} a_{i+1} = r(a_i - |a_i|^2) - rb_i, \\ b_{i+1} = -b_i e^{-2\beta} + e^{-\beta} r [(2 - a_i - a_i^*)b_i - a_i c_i^* - a_i^* b_i], \\ c_{i+1} = -c_i e^{-2\beta} + e^{-\beta} r [2(1 - a_i^*)c_i - 2a_i b_i - a_i], \end{cases} \quad (2)$$

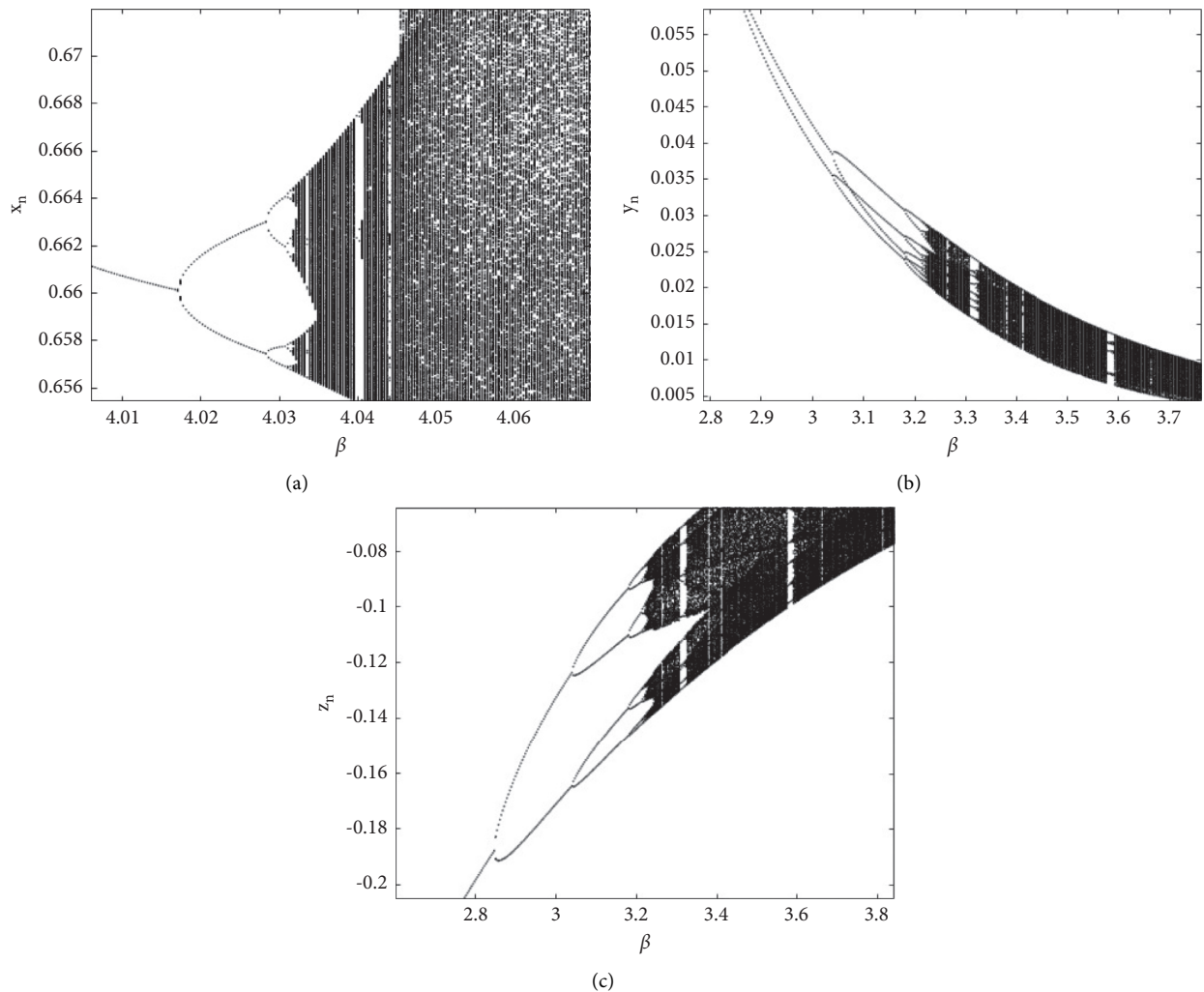
where  $a = p$ ,  $b = \delta a^\dagger \delta a$ ,  $c = \delta a \delta a$ , and  $\beta, r$  are bifurcation parameters. In general,  $a_{i+1}$ ,  $b_{i+1}$ , and  $c_{i+1}$  are all complex numbers, with  $a_i^*$  signifying the complex conjugate of  $a_i$  and  $c_i^*$  symbolizing the complex conjugate of  $c_i$ , respectively. If it is established that the initial values are real numbers, it can be concluded that all following values will also be real numbers. The logistic map with additive noise has the same shape as in equation (1) a. It should be mentioned that the noise is generated entirely by the computer system. The noise in this circumstance serves as a gauge for the strength of quantum correlations. The quantum corrections  $b_i$  and  $c_i \rightarrow \infty$  reduce equation (1) to the classical, one-dimensional logistic map in the presence of the quantum corrections. The resilient dissipation limit  $\beta \rightarrow \infty$  of the quantum logistic map also provides the classical logistic map, which is a further benefit. The quantum map depicts a road to chaos that doubles in length every period. When using an unsigned binary representation, the fixed point at 1 can be avoided by rounding down, whereas the fixed point at 0 is more difficult to avoid. Options include reseeding the circuit with a new randomly chosen initial condition (which must be coordinated with synchronized circuits), adding a constant value (which leads to known state conditions to any source that knows the constant and arithmetic precision), or limiting the valid range of chaotic parameter values so that the mapping cannot generate a value less than LSB/2 [25]. Figure 2 shows the bifurcation diagram of equation (1).

```

Input: key
Output: pseudorandom numbers sequence
(1) while value! = 0 and value is not reiterating,
  Do
(2) Bin  $\leftarrow$  attain the binary configuration of the Value.
(3) Pad until bin has 16 bits with leading zeros.
(4) XOR the bits at situations respective to LF function and save it in  $m$ .
(5) Bin  $\leftarrow$  shift the bin by one toward the right.
(6) Pad until bin has 16 bits with leading zeros.
(7) The first bit is replaced with  $m$  in the bin.
(8) Value  $\leftarrow$  attain the decimal value of the obtained binary configuration.
(9) End

```

ALGORITHM 1: Algorithm of Linear Feedback Shift Register.

FIGURE 2: Bifurcation diagram of parameters  $\beta$  at  $r = 3.88$  in (a)  $x$ -direction; (b)  $y$ -direction; (c)  $z$ -direction.

### 3. Proposed Encryption Algorithm

The combination of quantum chaotic map and LFSR is created for use in the encryption system that is being suggested. Using this function in combination with

word-based LFSR, it is possible to generate extremely high-quality pseudorandom numbers. In cryptography, developing a robust LFSR with extraordinary periodicity and great cryptological characteristics is a current research topic. This function can preserve a wide range of cryptographic

characteristics. The secret key generation, with the addition presented technique using encryption and decryption, is structured as follows:

**3.1. Key Generation.** The key generation of the proposed cryptosystem is completely dependent on the input of the encryption technique. The private key's dependency on plaintext makes it secure against chosen-plaintext attack, chosen-ciphertext attack, and known-plaintext attack. The two parts of encryption diffusion and key-based substitution depend on the plaintext-based key. The first part is the generation of the LFSR sequence for which the plaintext provides seed value. The produced LFSR sequences are diffused with the original image. The second part is the production of a quantum chaotic map-based key for key-based substitution. The chaotic map key is also plaintext dependent because the initial values of the differential equation set are induced by using input values.

Consider the size of the input image  $M$  is  $P \times Q \times 3$ . After separating the image into three layers, R, G, B, we get each layer of size  $P \times Q$ . The seed value for LFSR and initial conditions for the chaotic map is generated by

$$I = \frac{\sum_{i=1}^P \sum_{j=1}^Q P_i Q_j}{P \times Q}. \quad (3)$$

After inserting this value of  $I$  for image  $M$  the keys  $K_1$  and  $K_2$  are obtained by the LFSR and chaotic quantum map.

**3.2. Encryption and Decryption.** The encryption process of the presented structure follows the confusion and diffusion properties. Corresponding to Shannon's theory [26], a resilient cryptosystem must contain confusion and diffusion effects. To achieve robust security, the system is subjected to input-dependent key and confusion-diffusion strategies. The encryption strides are defined as follows:

*Step 1.* Read an image input  $M$  of size  $P \times Q \times 3$  and convert it into a red, green, and blue layer.

*Step 2.* Diffuse the original image layers secret key  $K_1$  obtained by seeding input image to LFSR.

*Step 3.* The image layers obtained in Step 2 are stored as diffused image  $D^I$ ,  $I = R, G, B$ .

*Step 4.* The key  $K_2$  obtained by chaotic quantum map by using the original image based initial conditions is utilized for substitution as follows:

Rule 1: if  $0 \leq k_2(ij) \leq 150$  then put  $c_{ij}^I = d_{ij}^I \oplus k_2(ij)$

Rule 2: if  $151 \leq k_2(ij) \leq 255$  then put  $c_{ij}^I = d_{ij}^I \oplus k_2(ij) \oplus a$

Here,  $a \in \mathbb{Z}_{256}$ , is any fixed constant selected randomly,  $d_{ij}^I \in D_{ij}^I$  is the pixel value of diffused image  $D^I$ ,  $k_2(ij)$  is the value of  $K_2$  and  $c_{ij}^I \in C_{ij}^I$  is the pixel value of the final cipher image  $C^I$ ,  $I = R, G, B$ , and position  $i$  and  $j$ , respectively.

The image  $C^I$ ,  $I = R, G, B$  is the diffusion-substitution-based cipher obtained from the presented strategy.

A clear description of the presented encryption is defined in Figure 3.

The decryption of the presented structure is based on a similar strategy in a reverse manner. The same key  $K_1$  is first diffused with the encrypted image. After that, the key  $K_2$  is utilized for the process of inverse substitution. The substitution rules are defined in a reverse manner as:

Rule 1: if  $0 \leq k_2(ij) \leq 150$  then put  $d_{ij}^I = c_{ij}^I \oplus k_2(ij)$

Rule 2: if  $151 \leq k_2(ij) \leq 255$  then put  $d_{ij}^I = c_{ij}^I \oplus k_2(ij) \oplus a$

Where  $a \in \mathbb{Z}_{256}$ , is any fixed constant selected randomly,  $d_{ij}^I \in D_{ij}^I$  is the pixel value of diffused image  $D^I$ ,  $k_2(ij)$  is the value of  $K_2$  and  $c_{ij}^I \in C_{ij}^I$  is the pixel value of the final cipher image  $C^I$ ,  $I = R, G, B$ , and position  $i$  and  $j$ , respectively.

The inverse of the diffusion process is computed by the following way:

$$M = D_{ij}^I \oplus K_1, \quad (4)$$

where  $M$  is the decrypted plain image.

## 4. Statistical Analysis of Recovered Image

Good encryption procedures should be resistant to a wide range of different attacks such as the differential, statistical attacks, and brute force attacks. We carried out a security analysis of our proposed scheme. The enciphered images yielded by the presented encryption structure are illustrated in Figure 4.

**4.1. Entropy.** Entropy analysis was performed to examine the randomness that can be used to define image texture and information content. It refers to the pixel's ability to detect various gray levels. Entropy is high if image pixels are uniformly scattered, while entropy is low in the case of the plain image. Scientifically it can be inscribed as

$$H(S) = - \sum_{i=0}^{255} p(s_i) \log_2(p(s_i)). \quad (5)$$

The numerical outcomes of the information entropy are displayed in Table 1. The results were calculated for plain and encrypted layers of some standard images with sizes.  $512 \times 512 \times 3$  From the listed results, it can be perceived that the entropies for enciphered images are near enough to the epitome value that is 8 compared to the original ones. Therefore, the presented scheme produces uniform ciphers with a higher value of entropy.

The entropy calculated above in Table 2 is the global entropy. The global Shannon entropy does not always measure actual randomness. Unlike global Shannon entropy, local Shannon entropy  $H_{(k,TB)}$  can capture local image block unpredictability, while global Shannon entropy cannot. The local entropy  $E_{(k,TB)}$  can be calculated as

$$\overline{H}_{(k,TB)}(S) = \sum_{i=1}^k \frac{H(S_i)}{k}, \quad (6)$$

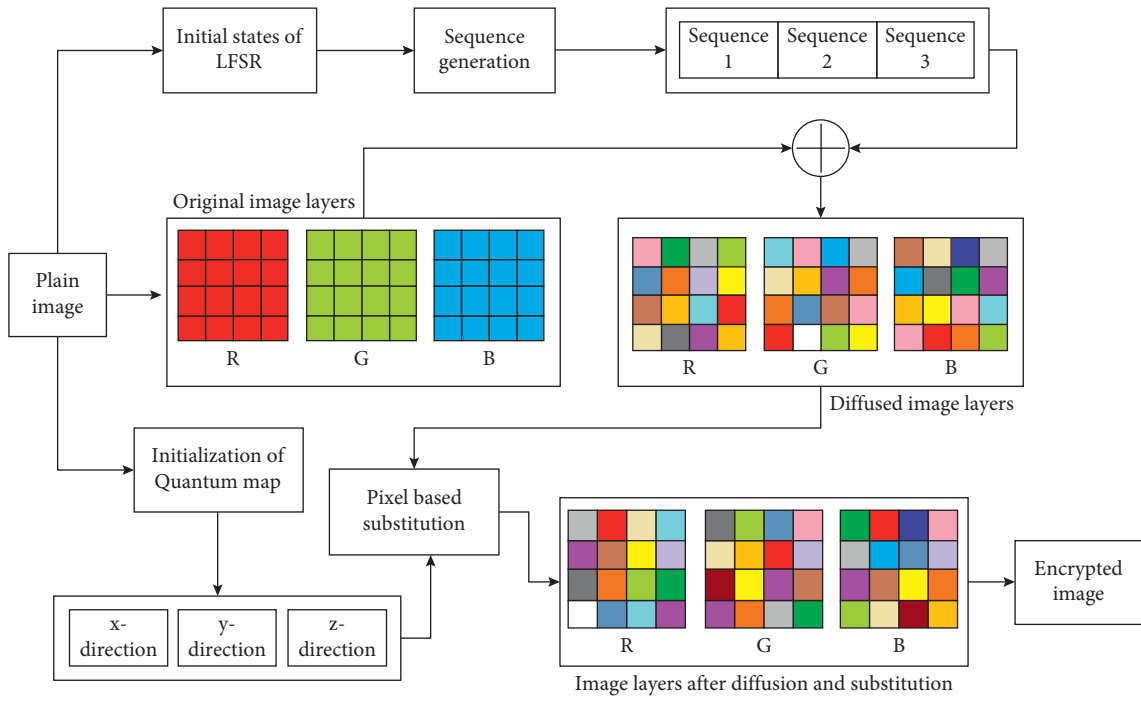


FIGURE 3: Design of presented encryption scheme.

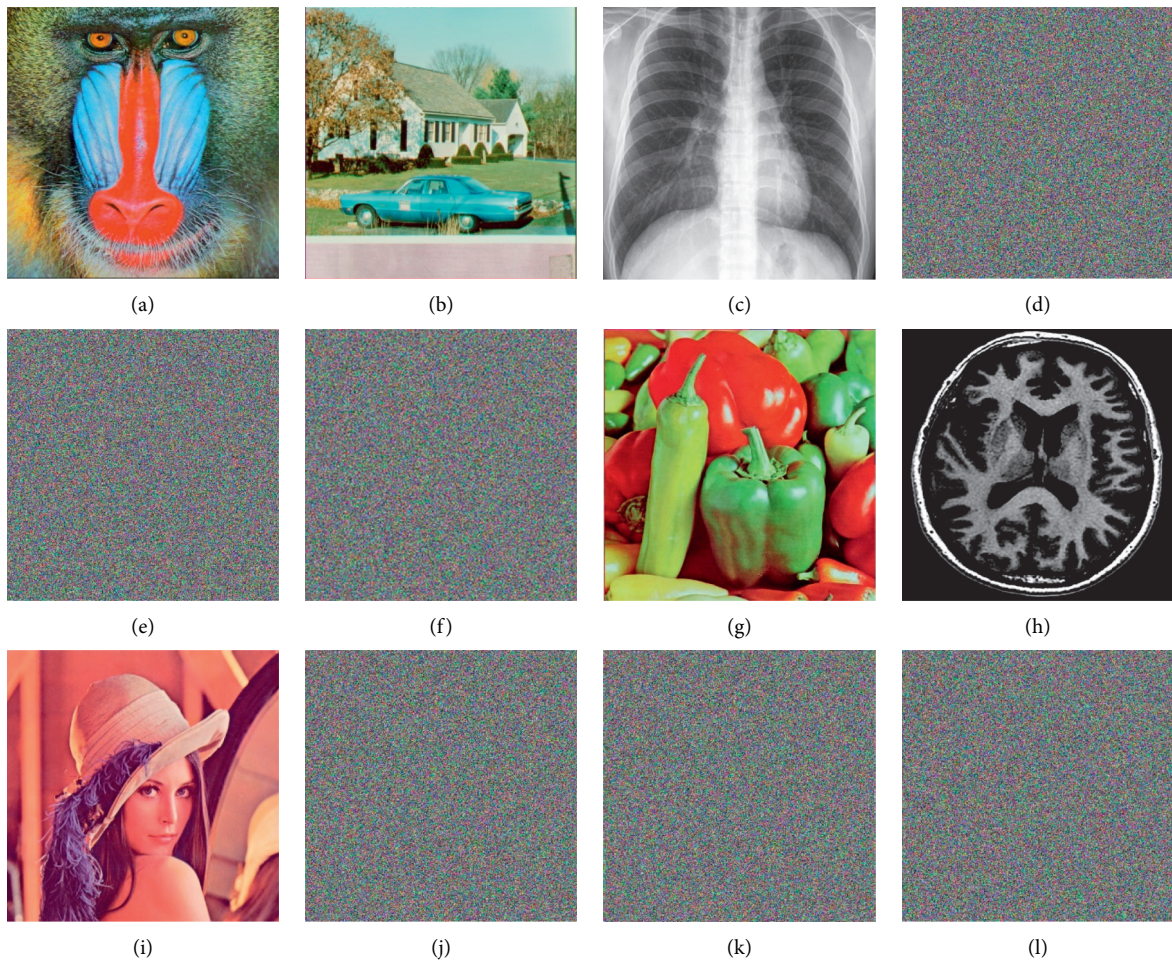


FIGURE 4: (a-c), (g-i) Original standard images of size  $512 \times 512$ ; (d-f), (j-k) Respective cipher images.

TABLE 1: Entropy measures for different images.

Image	Original image				Enciphered image			
	Color	R	G	B	Color	R	G	B
Baboon	7.7624	7.7067	7.4744	7.7522	7.9996	7.9992	7.9995	7.9991
Peppers	7.6698	7.3388	7.4963	7.0583	7.9998	7.9991	7.9983	7.9994
House	7.0686	6.4311	6.5389	6.2320	7.9986	7.9972	7.9986	7.9983
Brain	7.0156	7.0156	7.0156	7.0156	7.9991	7.9986	7.9989	7.9989
X-ray	7.2369	7.2369	7.2369	7.2369	7.9993	7.9993	7.9989	7.9996
Lena	7.7562	7.5889	7.1060	6.8147	7.9995	7.9990	7.9992	7.9993

TABLE 2: Local entropy measures for different sizes of Lena image.

$k$	Lena image		Entropy value		
	TB		R	G	B
16	$32 \times 32$		5.9635	5.8740	5.9954
32	$64 \times 64$		6.8951	6.0147	6.5214
64	$128 \times 128$		6.0589	5.9959	56.0028
128	$256 \times 256$		6.5230	6.5024	6.5804
256	$512 \times 512$		7.8111	7.8047	7.9852
512	$1024 \times 1024$		7.8974	7.9632	7.9841

where  $S_i$  denotes the nonoverlapping blocks of image  $S$ ,  $k$  shows the number of blocks, TB represents the total size of the image, and  $L$  shows the intensity of the pixels.

The calculation of local entropy of Lena image for different sizes of the image is shown in Table 2 which depicts the maximum randomness of the ciphers produced from the proposed algorithm.

**4.2. Histogram Analysis.** The distribution of pixel numerical information within any image can be revealed using histogram analysis. If the image histogram after the encryption is distributed uniformly, this is considered a robust encryption system. Featured image histograms show complete similarity and differ from the dynamic histograms of explicit images, which is important in resisting any cryptographic assault. The similarity to the grayscale of the embedded image proves that no practical information can be obtained when performing any mathematical attack on the compiled image. 3D color histograms for Brain images of size  $512 \times 512 \times 3$  are depicted in Figure 5. From Figures 5(a)–5(d), we can perceive the pattern of original data in histogram distribution, and in the case of encrypted ones Figures 5(e)–5(h), the distribution is uniform. Therefore, the presented encryption design is robust against all the linear and differential attacks due to the ideal uniformity in the encrypted data.

In addition to the visual examination of the encrypted image histogram distribution, we perform the chi-square test ( $\chi^2$ ) to prove that the encrypted image has a uniform histogram distribution more precisely. The  $p$  value of the chi-square test is a real number in the range  $[0, 1]$ . For a test image to pass, the  $p$  value must be larger than a significant level  $\alpha$ . Table 3 shows the  $p$  values for some standard cipher images encrypted by the proposed algorithm, using an a priori of 0.05. The cipher image has a uniform histogram distribution based on the results of the chi-square test in

Table 3. The depicted results show that the proposed approach accepts null hypotheses and confirms the uniformity of histograms.

**4.3. Correlation Analysis.** Pixel correlation is a frequent approach for measuring the picture encryption algorithm's performance. In the image, a secure encryption algorithm requires a reduction in the correlation of contiguous pixels. The subsequent formula is utilized to quantify the correlation between two neighboring pixels:

$$\gamma_{xy} = \frac{E((x - \mu_x)(y - \mu_y))}{\sqrt{\delta_x \delta_y}}, \quad (7)$$

where  $\mu$  is the expected value and  $\delta$  shows variance, the results obtained from correlation analysis are presented in Table 4. The values between two neighboring pixels are significantly lowered. The results show that the presented technique is resilient against different assaults as the correlation value is close to zero, so the scheme meets the standard criteria.

Figure 6(a)–6(f) depicts the scattering of neighboring pixels in various directions. The Lena image in Figures 6(a)–6(c) displays a substantial correlation among neighboring pixels for horizontal, vertical, and diagonal of the plain image. The correlation diagrams of the enciphered image are displayed in Figures 6(d)–6(f). The dots in the encrypted image are dispersed randomly, with no evident distribution features.

#### 4.4. Randomness Analysis

**4.4.1. NIST Test.** The NIST-800-22 trial was designed to test the pseudorandom number generator (PRNG). It can be examined that a complex binary sequence is appropriate for

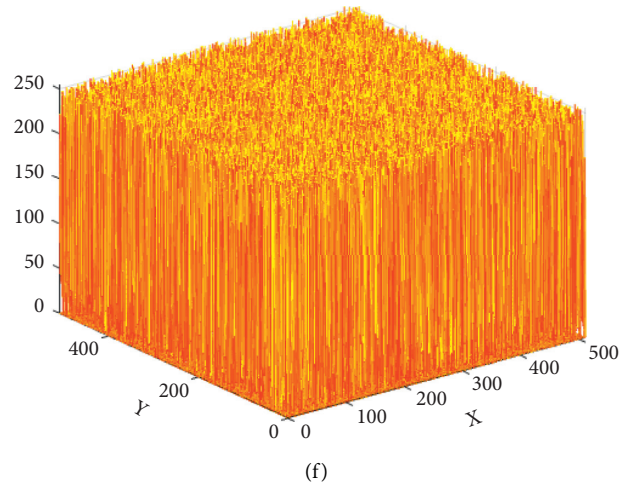
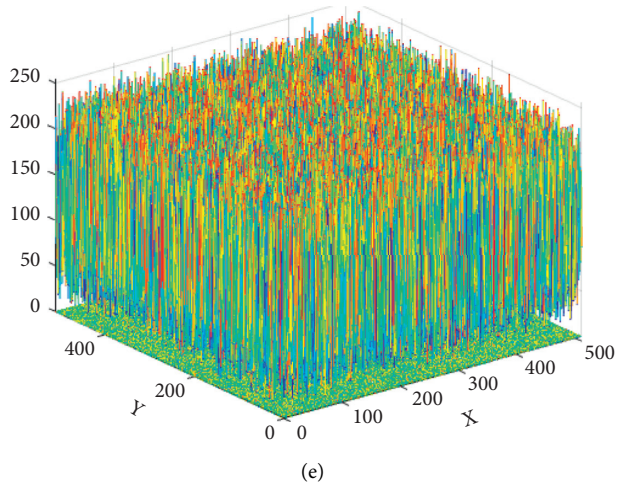
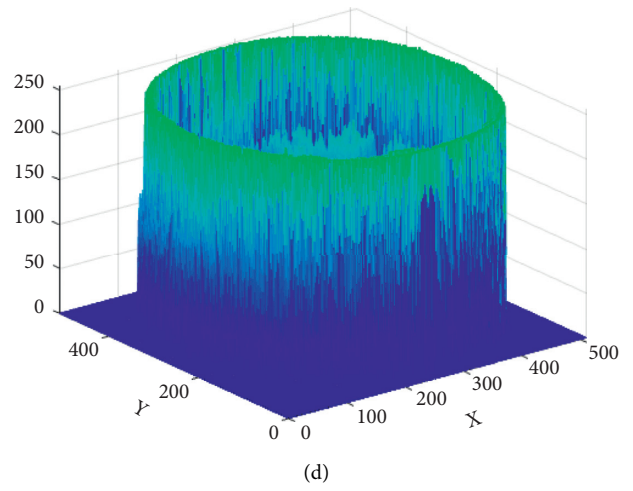
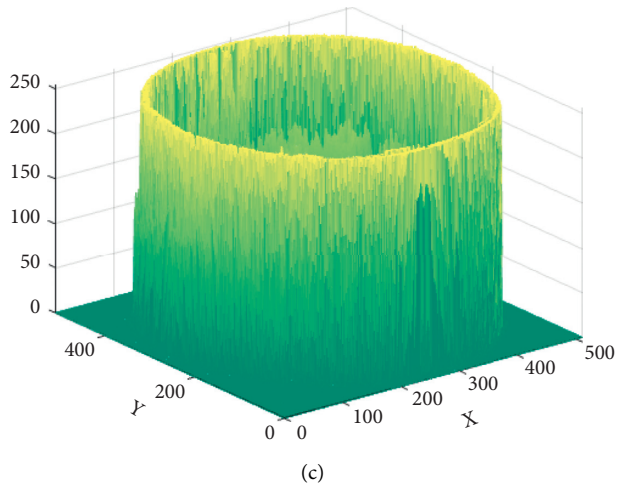
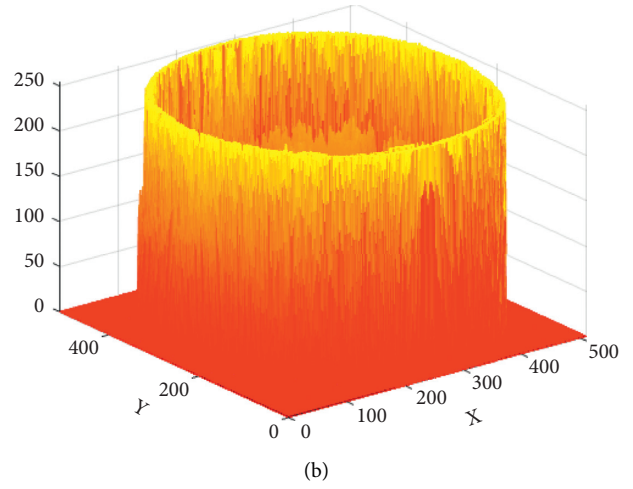
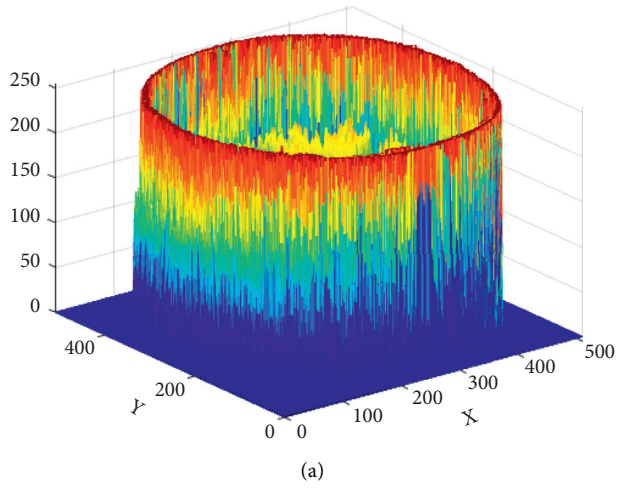


FIGURE 5: Continued.



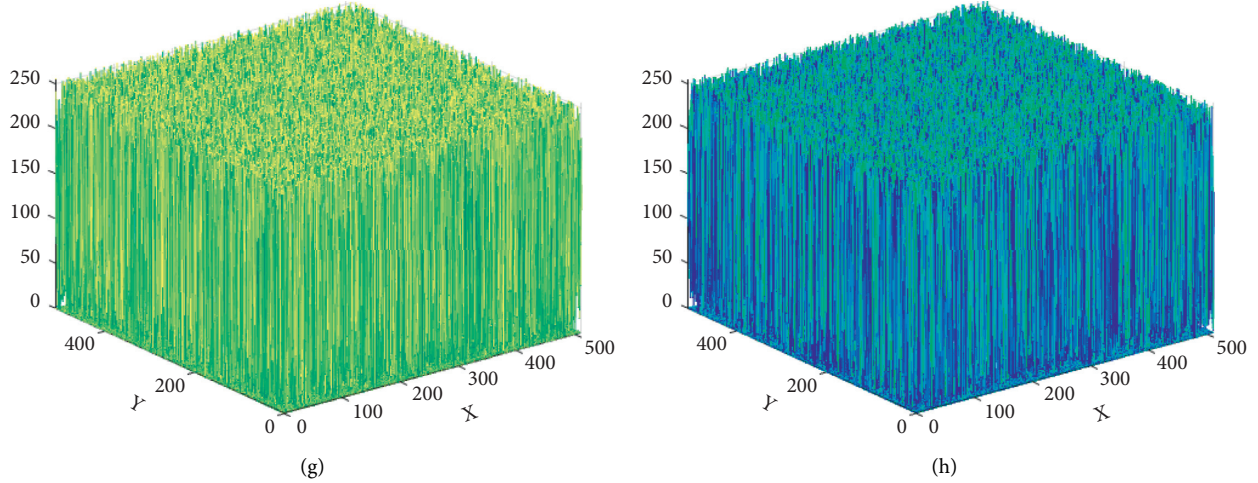


FIGURE 5: (a–d) 3D histogram of brain original image layers; (e–h) 3D histograms of brain encrypted image layers, respectively.

TABLE 3: Chi-square test measures for different images.

Image	Color	R	G	B
Baboon	0.4561	0.3698	0.4157	0.3687
Peppers	0.5151	0.9002	0.6958	0.2589
House	0.5102	0.0947	0.5179	0.4763
Brain	0.5089	0.8962	0.6527	0.6215
X-ray	0.4011	0.0940	0.8526	0.1258
Lena	0.0647	0.0871	0.9654	0.7521

TABLE 4: Correlation coefficient measures for enciphered images.

Image	Orientation	Encrypted		
		R	G	B
Baboon	Diagonal	-0.0001	-0.0009	0.0007
	Vertical	0.0002	0.0010	0.0010
	Horizontal	-0.0003	-0.0011	0.0001
Peppers	Diagonal	0.0043	0.0001	-0.0005
	Vertical	0.0013	-0.0003	-0.0004
	Horizontal	-0.0005	0.0002	0.0090
House	Diagonal	0.0014	-0.0015	0.0012
	Vertical	-0.0043	0.0014	-0.0054
	Horizontal	0.0015	-0.0002	0.0003
Brain	Diagonal	0.0032	0.0003	-0.0020
	Vertical	0.0011	-0.0002	-0.0010
	Horizontal	-0.0021	-0.0002	0.0003
X-ray	Diagonal	0.0004	0.0030	-0.0011
	Vertical	-0.0012	-0.0011	0.0040
	Horizontal	-0.0007	0.0012	-0.0056
Lena	Diagonal	0.0001	-0.0021	0.0003
	Vertical	-0.0001	0.0031	-0.0019
	Horizontal	-0.0031	-0.0011	0.0003

a cryptosystem based on the outcomes of the NIST test. The NIST-800-22 trial comprises 15 test approaches, comprising frequency test, run test, cumulative test, longest run test, etc. The number of  $p$  can measure the random sequence of the test sequence. If  $P \geq 0.01$ , the sequence is random. If  $P < 0.01$ , the sequence is nonrandom and predictable. If  $P = 1$ , the

structure is completely set. If  $p = 0$ , the structure is by no means random. In addition, the greater the  $p$  value; the better the random sequence. The results of NIST for chaotic sequences and some standard images are presented in Table 5. The depicted results reflect that the sequence generated from the chaotic map is highly random and ideal for encryption. The results can be scrutinized using the presented encryption algorithm that helps to generate highly random ciphers with  $P \geq 0.01$ .

**4.5. Differential Attack.** In the plain image, some pixels are faintly modified to attain the respective enciphered image. The opponent recurrently makes the connection between the encrypted images and the plain ones. If a small modification in the pixels of the image can significantly disturb the cipher image, it indicates that the structure has a resilient capability to withstand differential assaults. Differential attacks are usually inspected by the number of pixels change rate (NPCR) and unified average changing intensity (UACI) values [27, 28]. These two gauges are examined as follows:

NPCR is employed to enumerate plaintext sensitivity, i.e., the outcome of converting a lone pixel in the plain image into an encrypted image. It also describes the arbitrariness and modification among the original image and its respective cipher and can be written as

$$\text{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{w \times h} \quad (8)$$

The larger the value of NPCR, is better the original image sensitivity offered by the encryption algorithm. The UACI is defined as

$$\text{UACI} = \left[ \frac{\sum_{i=1}^w \sum_{j=1}^h |C_1(i, j) - C_2(i, j)|}{(2^8 - 1) \times w \times h} \right] \times 100\%, \quad (9)$$

where  $C_1$  is the first encrypted image and  $C_2$  is the second encrypted image, and  $w$  and  $h$  are the width and height of

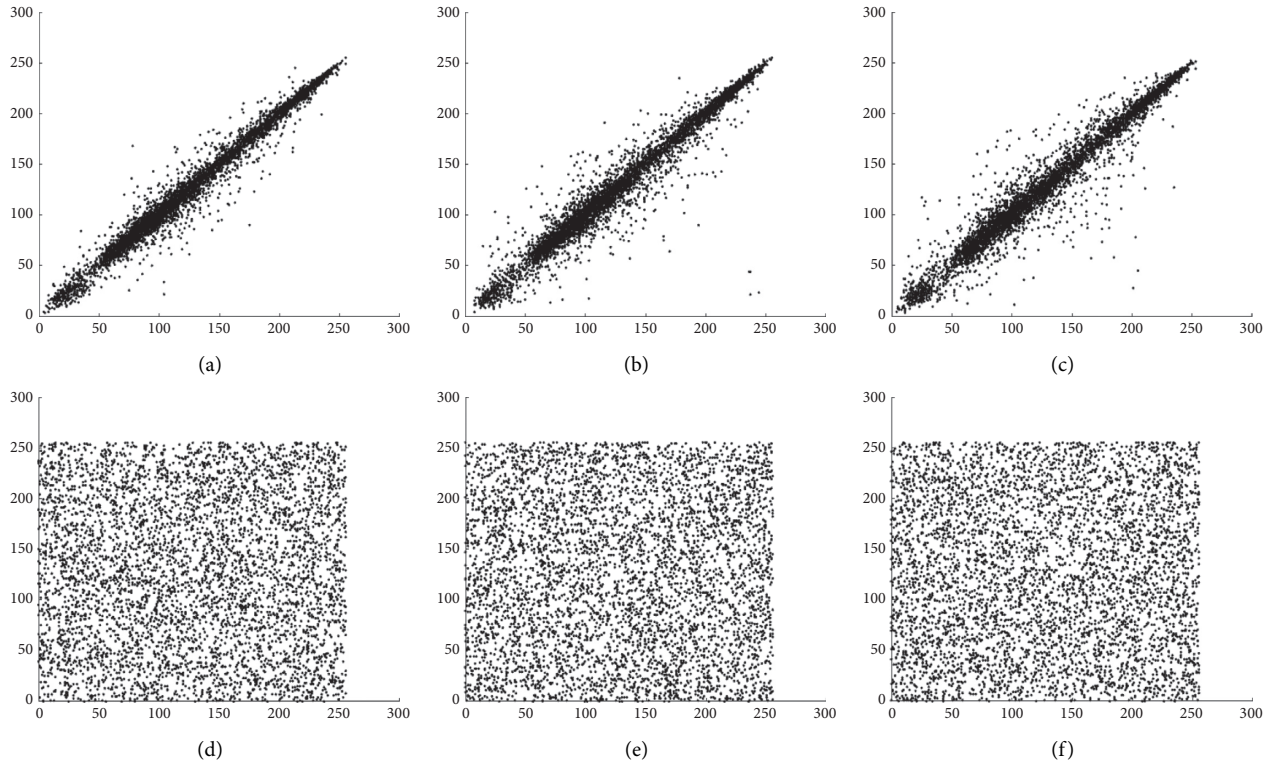


FIGURE 6: Correlation diagram of Lena original image in (a) horizontal direction; (b) diagonal direction; (c) vertical direction; correlation diagram of Lena encrypted image in (d) horizontal direction; (e) diagonal direction; (f) vertical direction.

cipher images  $C_1$  and  $C_2$ .  $2^8$  represents the number of bits in one pixel of red, green, and blue layers in a color image.

It can be observed from Table 6 that the results for NPCR and UACI are designated as over 99% and 33%, respectively. These results indicate that the suggested scheme can withstand differential attacks.

The strength of the algorithm against differential attack varies concerning the change in the size of input data [29]. Therefore, we have performed NPCR and UACI measures for different sizes of images to check the deviation of results. The results of NPCR and UACI for various sizes of Lena images are depicted in Table 7. The key generation of the offered encryption algorithm entirely depends on the input data. Therefore, a minor change in input refers to a large change in output. The data in Table 7 indicates that the algorithm resists differential attacks for various sizes of input data.

#### 4.6. Key Analysis

**4.6.1. Key Sensitivity Test.** In the encryption-decryption process, an ideal cryptographic algorithm must be sensitive to the private keys. To inspect the key sensitivity test, an enciphered image is deciphered using the different keys, which are one bit different from the correct key. Lena's standard color image of size  $512 \times 512 \times 3$  is evaluated for the test. Figure 7 depicts the results of this test and one can see that when the decryption key was only one bit different, the output (Figures 7(a), 7(b), and 7(c)) shows that it does

not reveal the contents of the original information. Figure 7(d) shows that decryption is possible only with the correct key.

**4.6.2. Brute Force Attack.** Space support is critical in countering a brute force attack. The authors of [1] proposed that the private keys of a cryptographic algorithm be greater than  $2^{100}$  to avoid Brute force attacks. To encrypt the plain image, a chaotic map seed value and a 256 bit key/seed value of a special LFSR to yield pseudorandom numbers are utilized. The proposed encryption system has a key space greater than  $2^{256}$  that is sufficient to withstand a Brute force attack. The integer value of the chaotic map when computing key space is not considered.

**4.7. Known and Chosen Plain Text Attacks.** Any cryptosystem with an excellent diffusion property is capable to withstand chosen and known-plaintext attacks. Overall, the opponent selects a distinct set of plaintexts consisting of sequential 0 and 1 data to demonstrate the algorithm's uncertainty. In the aforementioned attacks, plaintext and their corresponding ciphertext are selected. It permits our cryptosystem to produce enciphered images that are highly random.

The first step of the generation of encryption/decryption keys depends upon plaintext. The dependency of the algorithm on plaintext increases its security in contrast to chosen-plaintext attacks and chosen-ciphertext attacks. The substitution part of the suggested algorithm is also sensitive

TABLE 5: NIST measures for chaotic map and different standard color images.

Test name	P value				Status	
	Chaotic sequence	Baboon	Peppers	House		
Frequency	0.5632	0.7412	0.8191	0.8421	Pass	
Block frequency	0.0125	0.2156	0.0182	0.1355	Pass	
Runs	0.9523	0.1534	0.9542	0.9018	Pass	
Longest run	0.0357	0.0357	0.0357	0.0357	Pass	
Rank	0.2919	0.2919	0.2919	0.2919	Pass	
Serial 1	0.9635	0.8261	0.1144	0.6021	Pass	
Serial 2	0.8852	0.5963	0.7344	0.3740	Pass	
Cumulative sums	0.3562	0.3110	0.5810	0.5520	Pass	
Overlapping template	0.8899	0.9568	0.8625	0.8752	Pass	
Universal	0.7616	0.9981	0.9987	0.9986	Pass	
Approximate entropy	0.9523	0.2082	0.1342	0.7566	Pass	
Nonoverlapping template	0.8536	0.9989	0.9685	0.9452	Pass	
Random excursions	X = -4	1	0.9971	0.0114	0.1526	Pass
	X = -3	0.0563	0.2251	0.2586	0.3698	Pass
	X = -2	0.6677	0.3698	0.2589	0.0058	Pass
	X = -1	0.5147	0.9962	0.4411	0.6398	Pass
	X = 1	0.2431	0.8144	0.6325	0.9990	Pass
	X = 2	0.8891	0.0007	0.0081	0.5858	Pass
	X = 3	0.6974	0.5222	0.0014	0.0025	Pass
	X = 4	0.2547	0.0258	0.9981	0.0097	Pass
	X = -7	0.0145	0.1184	0.8894	0.0001	Pass
	X = -6	0.0021	0.0215	0.6235	0.0147	Pass
Random excursions variants	X = -5	0.5449	0.0523	0.7412	0.9638	Pass
	X = -4	0.1254	0.9632	0.9632	0.9965	Pass
	X = -3	0.8025	1	0.5258	0.1963	Pass
	X = -2	0.3698	0.0639	0.0258	0.6687	Pass
	X = -1	0.2250	0.0259	0.2649	0.2991	Pass
	X = 1	0.5896	0.9417	0.3258	0.3447	Pass
	X = 2	0.1569	0.2698	0.0143	0.7319	Pass
	X = 3	0.0147	0.6943	0.0984	0.7982	Pass
	X = 4	0.2589	0.5861	0.9584	0.9963	Pass
	X = 5	0.1267	0.9974	0.7463	0.2210	Pass
X = 6	0.0145	0.2255	0.8847	0.0009	Pass	
X = 7	0.0012	0.0006	0.3698	0.1717	Pass	

TABLE 6: NPCR and UACI measures for standard images.

Image	NPCR			UACI		
	R	G	B	R	G	B
Baboon	99.57	99.64	99.60	34.46	33.42	33.14
Peppers	99.62	99.69	99.63	33.43	32.44	33.32
House	99.63	99.64	99.62	32.50	33.43	34.52
Brain	99.74	99.70	99.63	33.49	33.47	33.37
X-ray	98.82	98.64	98.72	32.45	34.03	34.12
Lena	99.60	99.62	99.58	33.49	33.48	34.62

TABLE 7: NPCR and UACI measures for different sizes of Lena images.

Image	NPCR			UACI		
	R	G	B	R	G	B
128 × 128 × 3	99.01	98.90	99.30	32.21	32.95	32.01
256 × 256 × 3	99.70	99.60	99.80	33.36	33.58	33.44
512 × 512 × 3	99.66	99.54	99.64	33.40	33.49	33.61
1024 × 1024 × 3	99.67	99.63	99.63	33.95	33.60	33.69

to initial conditions because it changes with the respective plaintext. Therefore, in the presented structure, the chosen-plaintext and the chosen-ciphertext attack do not give any information about the secret keys of the system. As a result, the presented cryptosystem can efficiently endure chosen and known-plaintext attacks.

**4.8. Robustness Analysis.** While encrypted images are transported across the public network, one must take care of the noise issue. The noise enhancement may seem in modification, damage, and a condensed procedure of image data. The high level of noise creates it meaningfully tricky to retrieve the original images from the enciphered images. Therefore, repelling noise is an important benchmark to examine the strength of the cryptosystem.

To examine the strength of the presented encryption scheme two types of noises are added. The decrypted images are understandable though different types of noises were provided. From the decrypted image maximum information

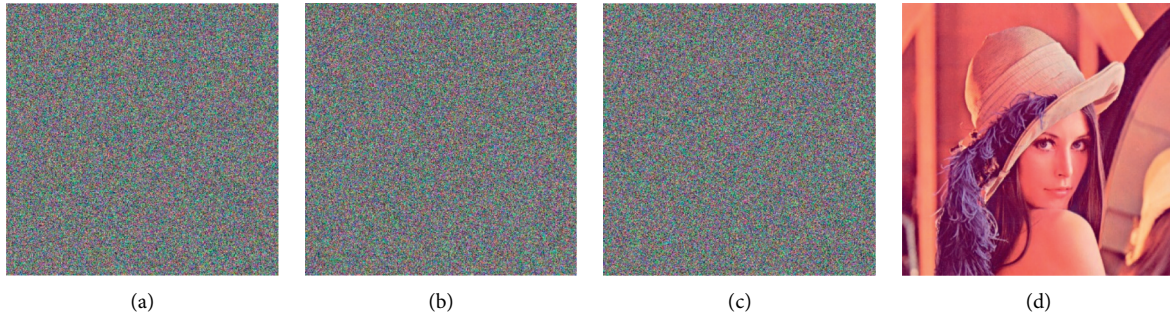


FIGURE 7: (a–c) Images decrypted from one-bit change key; (d) Image decrypted from the original key.

can be recovered. To check the quality of decrypted images, various tests are carried out such as peak signal-to-noise ratio (PSNR), mean-square error (MSE), homogeneity, and contrast.

**4.8.1. Mean Square Error (MSE).** MSE is a square measure of the error (pixel difference) of two images, obtained by taking a square root of a square error dispersed by the number of pixels in the image. Mathematically, it can be written as

$$\text{MSE} = \left[ \frac{1}{H * W} \sum_{y=0}^{H-1} \sum_{x=0}^{W-1} (f(x, y) - f'(x, y))^2 \right]^{1/2}, \quad (10)$$

where MSE is the mean square error, in image cryptography that means a larger number of MSE possess better image encryption capability. Average MSE values greater than 6000 for each channel are shown in Table 5 which depicts that the presented scheme is highly secure.

**4.8.2. Peak Signal to Noise Ratio (PSNR).** PSNR is defined as

$$\text{PSNR} = 10 \log_{10} \left( \frac{(255)^2}{\text{MSE}} \right), \quad (11)$$

a larger number of PSNR means better-deciphered images, and a smaller number means better image encryption.

The results of PSNR consequences of decrypted images with dissimilar levels of alterations are presented in Table 8. After incorporating numerous levels of noise concentrations in the encrypted image, it is perceived that the PSNR value reduces when noise concentration rises. The graphic excellence of the decrypted image is abridged, but the content is still noticeably predictable.

The PSNR value increases the fidelity of the encrypted picture to the original plain image [27]. When the PSNR is above 30 dB, it becomes difficult to distinguish between the original and decrypted pictures. The original Elaine test picture is encrypted twice. The resulting cipher pictures are then subjected to 33% data block loss, 99% data block loss, 0.005% Salt and Pepper noise, and 0.025% Salt and Pepper noise. Figures 8 show the outcomes for PSNR after including noise. In the  $3 \times 3$  data block loss test, the proposed method provides a PSNR of slightly under 35 dB (excellent quality).

TABLE 8: MSE and PSNR measures for different standard images.

Image	MSE			PSNR		
	R	G	B	R	G	B
Baboon	9231.2	8911.0	8952.3	39.6011	36.7412	39.3691
Peppers	9742.2	10356.1	11652.1	37.0031	48.8523	39.0001
House	7763.2	9954.1	7633.11	38.3737	29.5698	47.1102
Brain	6953.1	7836.2	8951.9	47.0186	37.8142	29.0997
X-ray	8642.2	9214.2	8686.1	39.1796	48.6981	59.1475
Lena	6651.4	9961.0	10029.2	39.7865	49.1345	39.1239

PSNR lowers to around 21 dB when testing for  $9 \times 9$  data block loss. A PSNR approaching 30 dB is achieved for the cipher image damaged by 0.005% Salt and Pepper noise. When the degradation reaches 0.02 percent, the PSNR nears 20 dB. Overall, the findings show that the suggested approach is somewhat robust to data loss and noise.

**4.9. Execution Time Analysis.** The speed at which an encryption-decryption method is executed is one of the most important quantifiable parameters. To determine the time for the presented system, three important processes are taken into consideration: parameter initialization, diffusion, and key-based substitution operation. Section 4 of this document contains a description of the presented system specification. Table 9 depicts the time requirements (in seconds) for encryption and decryption in this case. The demand for encryption and decryption time implies that the suggested algorithm is well-suited to dealing with a huge capacity of image data as compared to the existing results [30, 31].

Both the approximation of rounds as well as operations are required to achieve the enciphering and deciphering mechanism which is necessary to determine the computation difficulty. To estimate the computational complexity, the plain image had a dimension of  $M \times M$  is assumed. Initially, the pixel-level scrambling technique requires  $O(M \times M)$  time to complete. Following that, the keystream size is like the image size,  $M \times M$ , and  $O(M \times M)$  is known as the complexity of generation in nature. Finally, the diffusion operation requires  $O(M \times M)$ . As a result, the encryption approach has a total time complexity  $O(M^2)$ .



FIGURE 8: Data loss and noise attacks on encrypted images. (a) The untouched encrypted image and (b) its decrypted image; (c) the encrypted image with  $3 \times 3$  data block loss and (d) its decrypted image; (e) the encrypted image with  $9 \times 9$  data block loss and (f) its decrypted image; (g) the encrypted image deteriorated with 0.005% Salt and Pepper noise and (h) its decrypted image; (i) the encrypted image deteriorated with 0.02% Salt and Pepper noise and (j) its decrypted image.

TABLE 9: Time complexity analysis (in seconds) of offered structure.

Image size	Parameter initialization	Diffusion	Key-based substitution	Encryption	Decryption
$128 \times 128 \times 3$	0.050	0.198	0.311	0.559	0.418
$256 \times 256 \times 3$	0.191	0.224	0.298	0.713	0.691
$512 \times 512 \times 3$	0.283	0.356	0.489	1.128	0.918
$1024 \times 1024 \times 3$	0.412	0.517	0.511	1.440	1.3111

## 5. Comparison Analysis

Some of the critical performance measures, including key space analysis, the NPCR and UACI analysis, the correlation coefficient test for adjacent pixel analysis, and information entropy, are used to compare the performance of the suggested encryption scheme to that of current works in this section. Table 10 illustrates the comparison results between the given performance metrics of a Lena picture size

$256 \times 256 \times 3$  based on the suggested technique and the comparison results between existing methods. According to the tabulated results, the presented strategy outperforms the competition by a significant margin. One can see from Table 7 that the correlation in diagonal, horizontal, and vertical directions shows that the proposed scheme has significantly low correlation values when compared to other state-of-the-art encryption schemes. Therefore, our proposed algorithm is perfect because it comprises ideal

TABLE 10: Comparison of statistical results of the suggested scheme with existing work.

Features	Proposed	Ref. [32]	Ref. [11]	Ref. [12]	Ref. [13]
Key space	$2^{256}$	$2^{512}$	$2^{617}$	$2^{104}$	$2^{393}$
Diagonal correlation					
R	0.0001	-0.0060	-0.0026	0.0091	0.0167
G	-0.0021	0.0127	-0.0039	-0.0012	0.0171
B	0.0003	-0.0041	0.0012	0.0089	0.0170
Horizontal correlation					
R	-0.0031	-0.0033	-0.0029	0.0681	0.0021
G	-0.0011	-0.0067	-0.0032	0.0682	0.0023
B	0.0003	-0.0005	0.0040	0.0683	0.0024
Vertical correlation					
R	-0.0001	0.0055	0.0013	-0.0081	0.0017
G	0.0031	-0.0048	-0.0032	0.0040	0.0013
B	-0.0019	-0.0016	-0.0018	-0.0039	0.0011
NPCR					
R	99.60	99.51	99.60	99.87	99.57
G	99.62	99.53	99.61	99.88	99.56
B	99.58	99.54	99.61	99.89	99.57
UACI					
R	33.49	33.37	33.56	33.47	33.81
G	33.48	33.39	33.45	33.49	33.83
B	34.62	33.37	33.49	33.48	33.81
Information entropy					
R	7.9990	7.9992	7.9973	7.9953	7.9874
G	7.9992	7.9992	7.9969	7.9953	7.9871
B	7.9993	7.9992	7.9971	7.9953	7.9866

correlation values. NPCR and UACI of the proposed scheme are greater than 99.6 and 34, respectively. Our offered algorithm possesses perfect values of NPCR and UACI measures as compared to recently proposed work. The information entropy of the proposed scheme is near to the ideal value of 8 and it is also greater than other schemes. The greater value of information entropy as compared to other schemes indicates the robustness of the offered encryption algorithm. Through the comparison table, it is evident that the proposed scheme security is higher. However, the key space of the proposed scheme is lower than Reference [32], Reference [11], and Reference [13]. In the future, we will use coupled multi-chaotic maps for the higher key space.

## 6. Conclusion

Ensuring data security during the processes of communication and storage is mandatory these days as potential information leakage might have unwanted consequences. In this work, LFSR and chaos-based quantum map image encryption algorithm is presented. Both confusion and diffusion steps are utilized in the presented encryption. The proposed methodology can be used to encrypt images of different sizes. The entropy values of the encrypted images are significantly high when compared to the entropy values of original images. The presented scheme provides a security layer for images, and its effectiveness was validated through various experimental results such as key space and key sensitivity analysis. Furthermore, the proposed scheme has low correlation values and higher NPCR, and UACI test

results. The algorithm is resistant to most known attacks such as differential and statistical attacks etc. These security metrics prove that the proposed scheme achieved a higher security level, and it is well suited for digital image encryption for robust communications. The suggested technique has a low computing overhead and produces a secure ciphertext image within a few seconds. Our work can be further improved and modified to encrypt sensor data, biomedical data [33, 34] in the future. Furthermore, the system can be improved using the concept of parallelism to encrypt massive amounts of multimedia data.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Consent

Not Applicable.

## Conflicts of Interest

The authors declare no conflict of interest.

## Authors' Contributions

*Institutional Review Board Statement:* not applicable. *Human and Animals' rights.* This article does not contain any studies with human participants or animals performed by any of the authors.

## Acknowledgments

One of the authors, Sajjad Shaikat Jamal, extends his gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through a research group program under grant number R. G. P. 1/399/42.

## References

- [1] A. Churcher, R. Ullah, J. Ahmad et al., "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, 2021.
- [2] A. Qayyum, J. Ahmad, W. Boulila et al., "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, Article ID 140876, 2020.
- [3] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.
- [4] M. V. Berry, N. L. Balazs, M. Tabor, and A. Voros, "Quantum maps," *Annals of Physics*, vol. 122, no. 1, pp. 26–63, 1979.
- [5] N. L. Balazs and A. Voros, "The quantized Baker's transformation," *Annals of Physics*, vol. 190, no. 1, pp. 1–31, 1989.
- [6] M. Saraceno, "Classical structures in the quantized baker transformation," *Annals of Physics*, vol. 199, no. 1, pp. 37–60, 1990.
- [7] R. X. D. Schack and C. M. Caves, "Shifts on a finite qubit string: a class of quantum baker's maps," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 4–5, pp. 305–310, 2000.

- [8] N. Meenakshisundaram, *Studies in Quantum Chaos: From an Almost Exactly Solvable Model to Hypersensitive Operators*, Ph.D. thesis, Indian Institute of Technology Madras, Chennai, 2010.
- [9] S. Graffi and M. Degli Esposti, "The mathematical aspects of quantum maps," *Lecture Notes in Physics*, Springer, vol. 618, , 2003.
- [10] F. Haake, *Quantum Signatures of Chaos*, Springer, NewYork, NY, USA, 2000.
- [11] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.
- [12] P. Praveenkumar, N. Kerthana Devi, D. Ravichandran et al., "Transreceiving of encrypted medical image - a cognitive approach," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8393–8418, 2018.
- [13] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, 2014.
- [14] F. Masood, W. Boulila, J. Ahmad et al., "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sensing*, vol. 12, no. 11, p. 1893, 2020.
- [15] F. Masood, M. Driss, W. Boulila et al., "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Personal Communications*, pp. 1–29, 2021.
- [16] S. A. Shah, J. Ahmad, F. Masood et al., "Privacy-preserving wandering behavior sensing in dementia patients using modified logistic and dynamic Newton Leibniz maps," *IEEE Sensors Journal*, vol. 21, no. 3, pp. 3669–3679, 2021.
- [17] K. K. Butt, G. Li, F. Masood, and S. Khan, "A digital image confidentiality scheme based on pseudo-quantum chaos and Lucas sequence," *Entropy*, vol. 22, no. 11, p. 1276, 2020.
- [18] S. K. Bishoi, H. K. Haran, and S. U. Hasan, "A note on the multiple-recursive matrix method for generating pseudo-random vectors," *Discrete Applied Mathematics*, vol. 222, pp. 67–75, 2017.
- [19] G. Zeng, W. Han, and K. He, "High Efficiency Feedback Shift Register:  $\sigma$ -LFSR," 2007, <https://eprint.iacr.org/2007/114>. Cryptology ePrint Archive, Report 2007/114.
- [20] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 15605–15621, 2019.
- [21] Y. Dong, X. Huang, Q. Mei, and Y. Gan, "Self-Adaptive Image Encryption Algorithm Based on Quantum Logistic Map," *Security and Communication Networks*, vol. 2021, Article ID 6674948, 12 pages, 2021.
- [22] A. Ahmed, L. Abd El, L. Li, N. Wang, H. Qi, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.
- [23] R. Graham, T. Tel, and S. Isermann, "Quantization of Hanon's map with dissipation," *Zeitschrift für Physik B Condensed Matter*, vol. 60, no. 2–4, pp. 127–136, 1985.
- [24] M. E. Goggin, B. Sundaram, and P. W. Milonni, "Quantum logistic map," *Physical Review A*, vol. 41, no. 10, pp. 5705–5708, 1990.
- [25] A. J. Michaels, "Quantitative comparisons of digital chaotic circuits for use in communications," *Proceedings of the Joint INDS'11 & ISTET'11*, vol. 11, pp. 1–8, 2011.
- [26] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [27] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics & Laser Technology*, vol. 114, pp. 224–239, 2019.
- [28] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.
- [29] Y. Wu, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Journal of Selected Areas in Telecommunications*, pp. 31–38, 2011.
- [30] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.
- [31] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, Article ID 103056, 2021.
- [32] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8629–8652, 2018.
- [33] J. Masood, M. Shahzad, Z. A. Khan et al., "Effective classification algorithms and feature selection for bio-medical data using IoT," in *Proceedings of the 2020 Seventh International Conference on Information Technology Trends (ITT)*, pp. 42–47, IEEE, Abu Dhabi, UAE, November 2020.
- [34] K. Driss, W. Boulila, A. Batool, and J. Ahmad, "A novel approach for classifying diabetes' patients based on imputation and machine learning," in *Proceedings of the 2020 International Conference on UK-China Emerging Technologies (UCET)*, pp. 1–4, IEEE, Glasgow, UK, August 2020.