İSTANBUL UNIVERSITY CERRAHPAŞA

REVIEW
Electrica 2025; 25: 1-13

Image Encryption Using Quantum Logistic Mapping

Meryem Kılıç, Mustafa Cem Kasapbaşı

Department of Computer Engineering, İstanbul Ticaret University Faculty of Engineering, İstanbul, Türkiye

Cite this article as: M. Kılıç and M.C. Kasapbaşı, "Image encryption using quantum logistic mapping," *Electrica*, 25, 0059, 2025. doi: 10.5152/electrica.2025.25059.

ABSTRACT

With the growth of technology, the issue of safe storage and transmission of information has become even more important. Image data are increasingly used in military, business, political, economic, and other areas. The range of usage has increased, leading to increased privacy and security concerns about image data. In this study, it is aimed to present a new secure image encryption algorithm that leverages chaos theory and chaotic maps. As quantum logistic maps are sensitive to initial conditions, a new stream encryption algorithm using quantum logistic maps has been proposed to encrypt color images. In order to obtain chaotic behavior and confusion, quantum logistic map values, image values, and already encrypted values are utilized together to obtain both confidentiality and avalanche effect. Moreover, to check the efficiency of the algorithm's performance, NIST statistical tests, histogram analysis, key sensitivity tests, correlation analysis, and information entropy tests are successfully performed. It is concluded that the proposed algorithm secures the communication among parties.

***Index Terms*—**Chaos, decryption, image encryption, quantum logistic map

I. INTRODUCTION

Secure communication is important to ensure the flow of information while protecting the confidentiality of data. Designing privacy systems is a technological challenge [1]. With the increase in internet usage, ensuring data security has become more important. Technological developments have also increased the use of multimedia data, which mainly includes image data. Images themselves may contain confidential information and therefore need to be encrypted and secured. Traditional algorithms such as advanced encryption standard and data encryption standard are effectively used when encrypting text data. Unlike textual data, image data have features such as high data capacity, more processing power and time required when encrypting in real-time applications, and strong correlation between pixels. Due to these features, encryption with traditional algorithms on image data is insufficient to hide the data. Although there are different image processing methods in the literature, image encryption algorithms using chaos and quantum behavior are the subjects of the research.

Chaos is the mathematical discipline that allows the behavior of disorder to emerge. Henri Poincaré is one of the important people who laid the foundation of chaos theory with the three-body problem. Edward Lorenz [2], while working on weather forecasting, found that small changes in initial conditions can have large consequences over time. He called this the butterfly effect. Recently, the initial value and parameter sensitivity properties of chaos theory have led to widespread use in the field of image encryption [3].

II. QUANTUM PRINCIPLES AND THEIR PLACE IN CRYPTOLOGY

Quantum physics emerged in the late 19th and early 20th centuries when classical physics became inadequate in subatomic issues. Developments in quantum physics have gone beyond the definitions of light and matter in classical physics. While light only exhibits wave properties in classical physics, quantum physics exhibits both wave and particle properties. German physicist Max Planck introduced the concept of "quantum" in the 1900s to explain the relationship between light and energy. He suggested that the energy levels of light were not continuous but in packets. The concept of "discontinuity" entered the physics literature with Planck.

Quantum mechanics is based on quantum principles. These are quantization, wave-particle duality, superposition principle, uncertainty principle, wave function, entanglement, and Pauli

Corresponding author:
Meryem Kılıç

E-mail:
mkilic@ticaret.edu.tr

Received: February 27, 2025
Revision Requested: March 31, 2025
Last Revision Received: May 14, 2025
Accepted: May 19, 2025
Publication Date: July 28, 2025

DOI: 10.5152/electrica.2025.25059

exclusion principle. The principle of quantization states that energy is not continuously distributed but in discrete packets [4]. Wave-particle duality emphasizes that subatomic level particles do not exhibit only particle or only wave behaviour as emphasised in classical physics but can exhibit both wave and particle properties [5]. Superposition is the existence of quantum particles in more than one state at the same time [6]. The Heisenberg uncertainty principle states that it is not possible to measure the position and momentum of an object at a certain moment at the same time [7]. The wave function determines the behavior of an object. In 1926, Max Born proposed that the absolute square of an object's wave function gives the probability of finding that object at a particular location. Entanglement means that quantum particles are connected even if they are not physically connected, which explains non-local correlations between particles such that the measurement on one determines the state of the other instantly, regardless of distance. The Pauli exclusion principle explains that no two fermions in a quantum system can be in the same quantum state. These principles are the foundation for the probabilistic and non-deterministic nature of quantum dynamics, compared to deterministic trajectories in classical nonlinear systems [8, 9].

The first example of using quantum physics in encryption in the literature is Stephen Weisner's quantum money study. These principles are used when quantum physics is applied in cryptography. One of the most secure communication methods is quantum key distribution. Quantum key distribution is an encryption method based on the principles of quantum mechanics. In classical numerical computing, information is expressed in bits of 0 or 1, whereas, in quantum computing, the unit of information is the quantum bit, or qubit. Cubits can be in two states at the same time. This situation is explained by the principle of superposition. The superposition state of qubits provides access to a very large computational area that can solve many problems with great computational complexity and supports the power of quantum computing, which can handle very large dataset problems with only a small number of qubits [10]. It is not possible to copy quantum states. Because the quantum system will collapse as soon as the quantum state is copied. Quantum money study was also created by taking advantage of this situation. The purpose of encryption is to prevent the transmitted data from being obtained by third parties while passing through the transmission channel. When the data in the transmission channel is interfered with, the data will be corrupted because the quantum system will collapse. It will be understood that the system has been intervened. As the importance of the confidentiality of image data increases, researchers have started to show interest in quantum methods for encrypting image data. After the development of quantum information theory and quantum computations, most of the quantum representations of images have begun to be made with the help of a lattice consisting of qubits [11].

Quantum mechanics' unique properties make it highly suitable for establishing secure keys between two parties. Mainly, quantum measurement and state randomness can be used for generating genuinely random bits. Secondly, entanglement provides for the simultaneous existence of the same string of random bits at two distant locations. Third, as opposed to classical bits, quantum forms cannot be exactly copied. An attacker has to settle for continuing to work on the quantum growth, in which case, he will introduce detectable changes to the quantum state. He will know this faulty attack prior to it occurring [12]. Quantum cryptography provides information security through the laws of physics.

Within this quantum framework, the quantum logistic map has been a desirable model with which to explore the intersection of nonlinear dynamics and quantum computation. Derived by quantizing classical logistic map schemes, the quantum logistic map brings in superposition through the utilization of quantum states and unfolds via unitary operators rather than real-valued recurrence relations. This quantum equivalent possesses not only critical features of classical chaos under certain parameterizations but also has novel behavior due to interference and quantum coherence [13]. From investigations of the dynamical features of such quantum maps, researchers seek to improve the understanding of classical chaos onset or suppression within quantum domains and advance the broader field of quantum chaos and quantum information theory.

Although a proper definition of it has not yet been formalized to differentiate it from its classical counterparts. Dissipative quantum maps can be defined by sensitive dependence on initial conditions, similar to classical maps. Based on this property, a proposal for an image encryption scheme via a quantum logistic map is presented [14].

In this study, the proposed encryption algorithm based on the Quantum Logistic Map is tested on color images. A Fractional-Order Improved Quantum Logistic Map is an improved version of a quantum logistic map utilized in this study [15]. The evaluations are conducted using the National Institute of Standards and Technology (NIST) randomness test suite. The next section provides an overview of the related literature, while the material and method section details the proposed algorithm and presents the results of the applied metrics. The evaluation and discussion section includes a comparative analysis of the proposed algorithm. Finally, the conclusion section interprets the obtained results and summarises the overall findings of the study.

III. LITERATURE REVIEW

In [14], a new method for encrypting images using the Quantum Logistic Map is proposed. In that study, the difference in the encryption process in the study values generated by the Quantum Logistic Map after converting to an integer, directly used for encryption, no 3D feature of the map is utilized.

In [16], the authors proposed a three-tier quantum encryption scheme designed to encrypt images. The algorithm integrates the Arnold transform and logistic map, incorporating block and bit-level permutations alongside pixel-level diffusion. This three-layered encryption approach enhances security performance, randomness, and efficiency.

In [17], a quantum image encryption scheme employing intra-bit and inter-bit level permutations based on logistic maps has been introduced. The scheme leverages the entanglement and superposition properties of quantum physics to bolster encryption security. Intra-bit and inter-bit permutations simultaneously alter pixel positions and grey values of the pixels. Additionally, the logistic map expands the key space, making the encryption more resilient to attacks.

In [18], a quantum image encryption scheme utilizing the quantum logistic map and a binary system is proposed. By combining quantum mechanics and chaos theory, a secure encryption algorithm is introduced. A high degree of sensitivity is achieved through two chaotic logistic systems and even a small change in the key results in significant differences in the encrypted image.

In [19], a chaotic image encryption scheme employing block-level and bit-level permutation techniques is proposed for secure image transmission. The Henon map is used as the chaotic mapping function. The imaging scheme is based on the Butterfly Network Topology. The security of the encryption process is ensured by applying a diffusion process through the definition of a unique initial vector for each image. In addition to various security analyses, the algorithm's security level has been evaluated through differential cryptanalysis.

In [20], the authors conducted a study on image encryption using a chaotic system. Working with large data sizes while performing bit-level scrambling can slow down encryption speed and reduce efficiency. To address this issue, an algorithm has been proposed that enables parallel processing during bit-level permutation. This algorithm uses four threads to shuffle eight-bit-plane simultaneously. Since the threads operate in parallel, the encryption time is significantly reduced, and the overall encryption efficiency is enhanced.

In [21], an image encryption method based on block-based transformation is proposed. This work includes both an image encryption algorithm and an image hiding technique. The image data is divided into small blocks and each block undergoes an XOR (Exclusive Or) operation with a secret key. The Blowfish encryption algorithm based on a chaotic standard map is employed for encryption. After the encryption process, it is observed that the correlation between pixels is significantly reduced. Furthermore, it was found that reducing the block length and increasing the number of blocks further diminished the correlation between pixels.

In [22], the authors conducted a study on quantum image encryption and decryption. It is emphasized that quantum image geometric transformations must be applied to enable quantum image encryption and decryption. First, the classical image must be represented as a quantum grayscale image. Next, the process of transferring the image to quantum computers is discussed. Finally, the transmitted image is securely encrypted, ensuring high accuracy during decryption. The paper explains how quantum algorithms are more secure and resilient than classical methods.

In [23], the authors proposed an asymmetric image encryption scheme using a quantum logistic map and cyclic modular propagation. The limitations and vulnerabilities of existing image encryption methods are discussed, and it is shown that using quantum technology in cryptography results in a more secure and cost-efficient system. The quantum state is introduced into a chaotic system to create a quantum logistic map, which increases randomness and makes the algorithm more robust. The RSA (Rivest-Shamir-Adleman) algorithm is used to determine the initial values of the quantum logistic map. The image blending process is performed with the Arnold map, followed by the XOR operation. This method aims to protect against various attacks by maintaining a high level of security.

In [24], a chaos-based encryption algorithm is proposed, using two logistic maps to perform confusion and propagation operations. The first logistic map scrambles pixel positions, while the second changes pixel values. This reduces the correlation between neighboring pixels and makes it difficult for third parties to intercept the encrypted image. Secure and fast encryption is achieved even for images with little information.

In [25], an algorithm is developed that uses a chaotic logistic map and an 80-bit key to encrypt data determined by the result of the logistic map. In this study, the data to be encrypted is divided into blocks, and a different private key is used for each block, enhancing the security of the encryption.

In [26], a self-adaptive image encryption algorithm was proposed based on the Quantum Logistic Map. As the randım sequence utilized in image encryption requires strict randomness, and the random sequence produced directly by the Quantum Logistic Map does not yield a good performance a preprocessing step was proposed for such random sequences.

IV. MATERIALS AND METHODS

This section describes the logistic map, quantum logistic map, and the proposed algorithm for image encryption. Measurements were conducted to assess the reliability of the image encryption flowchart and to analyze performance. For experiments, images were selected from the database [27], and the results are presented in the following section.

A. Logistic Map

Chaotic maps are a branch of mathematics that generates random states in dynamical systems, which are sensitive to initial conditions and exhibit a disordered, complex appearance [28]. The logistic map is commonly used as a chaotic map in cryptography and random number generation. Its mathematical expression is provided in (1).

$$x_{t+1} = r x_t \left(1 - x_t\right) \tag{1}$$

The unknown values in the mathematical expression of the logistic map must satisfy $0 < r < 4$, $t = 0, 1,2\ 3, \ldots$ ve $x \in (0, 1)$. For the map to exhibit chaotic behavior, the parameter r must lie within the range $3{,}57 < r < 4$ [29]. Fig. 1 illustrates the bifurcation diagram and the chaotic region of the logistic map.

The Lyapunov exponent is a tool used to measure the sensitivity of a chaotic map to small changes in initial conditions and control parameters [30]. A positive Lyapunov exponent indicates that the map exhibits chaotic behavior. The Lyapunov exponent of the logistic map is shown in Fig. 2. Since the Lyapunov exponents are positive, it is evident that the map is chaotic. The mathematical expression of the Lyapunov exponent is given in (2).

$$L = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \log\left|f'\left(x\right)\right| \tag{2}$$

B. Quantum Logistic Map

The logistic map is not suitable for high-security applications because it is one-dimensional and non-continuous. Therefore, we require quantum and multi-dimensional effective schemes so that the chaotic structure may be defined in a more complicated structure.

This section introduces the quantum logistic map and provides the corresponding equations. The concept of the quantum logistic map was first introduced in the literature by Goggin et al. 1990 [31]. The mathematical expressions for the three-dimensional quantum logistic map are presented in (3), (4), and (5).

$$x_{n+1} = r\left(x_n - |x_n|^2\right) - r y_n \tag{3}$$

$$y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r\left[\left(2 - x_n - x_n^*\right) y_n - x_n z_n^* - x_n^* z_n\right] \tag{4}$$

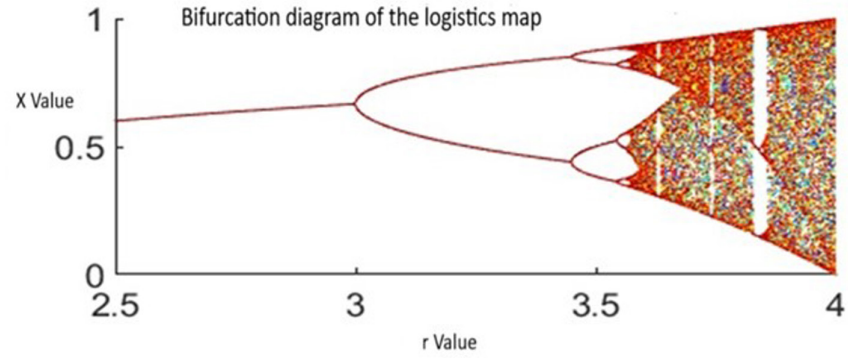


Fig. 1. Bifurcation diagram of logistics map.

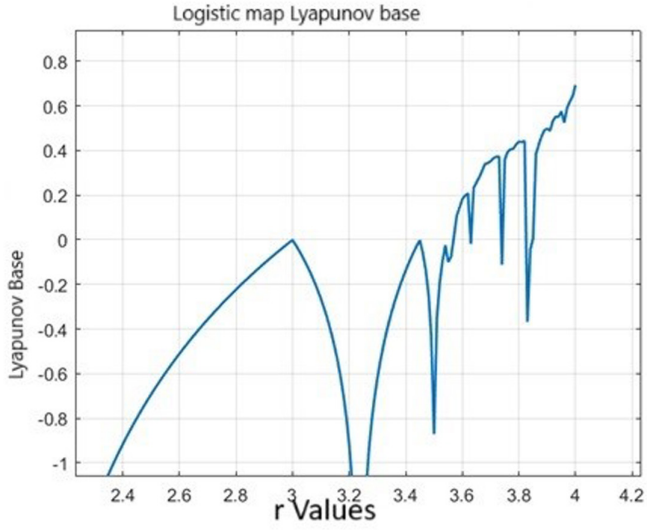


Fig. 2. Logistic map lyapunov base.

$$z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r\left[2\left(1-x_n^*\right)z_n - 2x_n y_n - x_n\right] \quad (5)$$

In these equations, β represents the dispersion parameter and r denotes the control parameter. The variables x^* and z^* are the complex conjugates of x and z, respectively. The parameter values lie within the following intervals $x \in [0, 1]$, $y \in [0, 0.1]$, $z \in [0, 0.2]$, $\beta \in [6, \infty]$, and $r \in [0, 4]$ [20]. Fig. 3 presents the phase diagrams of the quantum logistic map.

The novel quantum logistic map suggested by Xu et al. (2023) is introduced with the classical three-dimensional chaotic system. Equations 6 and 7 are referenced from [15]. Aside from nonlinearity, the model entails quantum currencies and fractional programming.

$$f(x) = \begin{cases} 0.8 + rx(0.2 - x), if\ 0 < x < 0.2 \\ r(x - 0.8)(1 - x), if\ 0.8 < x < 1 \end{cases} \quad (6)$$

$$x_{n+1} = f(x_n) - ry_n \quad (7)$$

This form enables the system to display various kinds of chaotic dynamics at specified intervals and creates a structure that has no equilibrium point, unlike the conventional chaotic system. This characteristic renders the system a hidden attractor chaotic system and makes it more unpredictable. Fig. 3 presents the phase diagrams of the quantum logistic map [15]. The phase diagram shows the behaviour of the system with respect to the initial conditions.

The three-dimensional quantum logistic map algorithm [15] has been modified to improve the efficiency of session key generation. Fig. 4 presents the phase diagrams resulting from this modification.

C. Proposed Encryption Algorithm

The proposed encryption algorithm is applied to color image data. The image, in a two-dimensional PNG file format, is converted into a one-dimensional byte stream. The three-dimensional quantum logistic map is executed using the initial values, and a session key for encryption is generated. The generated session keys must correspond to the size of the image. The encryption process is carried out, resulting in the encrypted image. During these operations, both scrambling and spreading techniques are applied. The steps of the proposed encryption algorithm are outlined below.

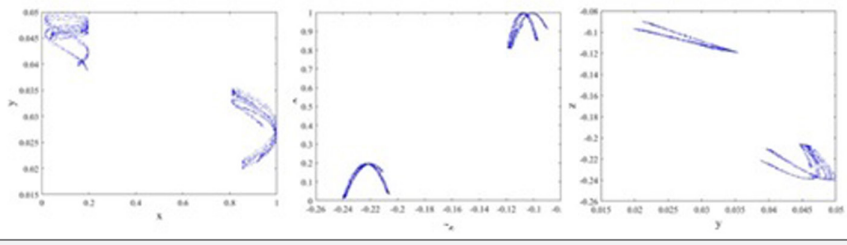


Fig. 3. Quantum logistic map phase diagrams. (a) xy plane; (b) yz plane; (c) xz plane.

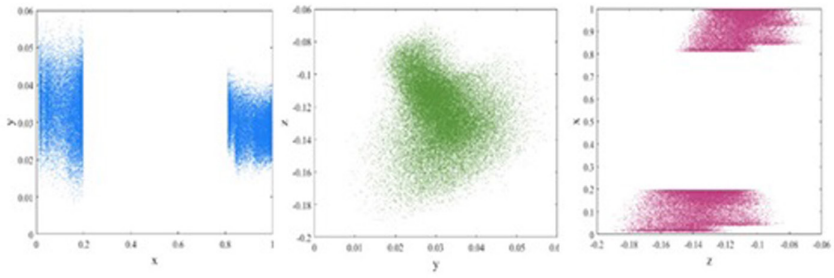


Fig. 4. Modified quantum logistic map phase diagrams. (a) xy plane; (b) yz plane; (c) xz plane.

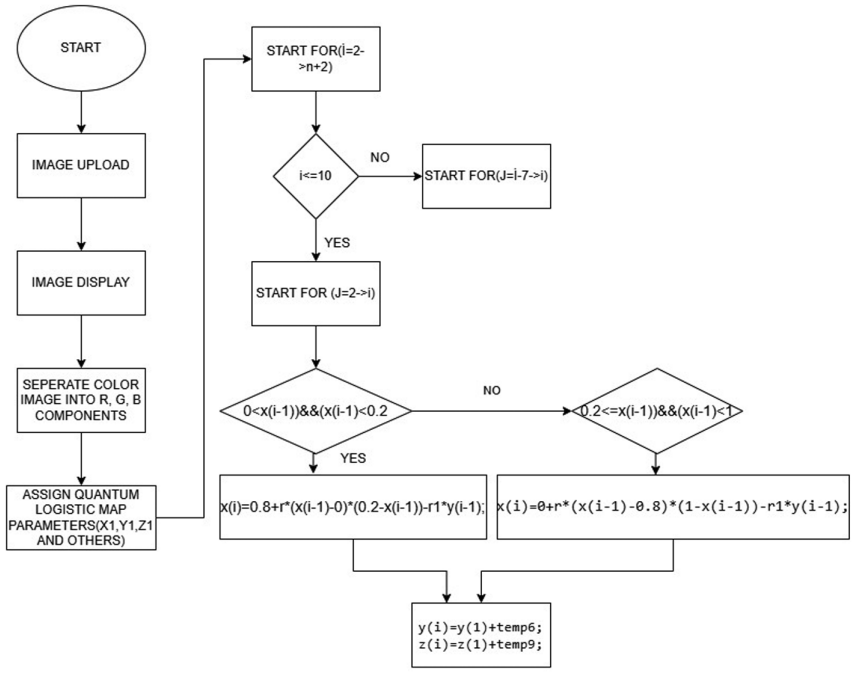


Fig. 5. Block diagram of the proposed quantum logistic map.

The quantum logistic map possesses a basic structure, high information-carrying capacity, and natural parallelism. Further, the produced chaotic sequences are more pseudo-random [23]. The quantum logistic map demonstrates superior chaotic behavior when $r = 3.99$ and $\beta \geq 6$. Initial values of x_1, y_1, and z_1 are assigned. Three random sequences are generated using the initial keys x_1, y_1, and z_1, three chaotic sequences.

Step 1: Initiating the process.

In this step, the $M_{m\times n\times p}$ sized image with ".Png" extension is read by the program.

Step 2: Image transformation.

The input image is reshaped, resulting in a one-dimensional vector. The image of size $M_{(m\times n\times p)}$ is converted into a string of size $M_{(m\times n\times p)\times 1}$.

Img_1d ← reshape (image, 1, [])

Step 3: Setting the initial parameters.

TABLE I. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY STATISTICAL TEST RESULTS

Test	*P*	Result
Frequency	.5341	Successful
Block frequency	.7399	Successful
Cumulative sums	.5341	Successful
Runs	.5341	Successful
Longest run	.7399	Successful
Rank	.3504	Successful
FFT	.3504	Successful
Universal	.00	Failed
Approximate entropy	.0668	Failed
Random excursions	–	Failed
Random excursions variant	–	Failed

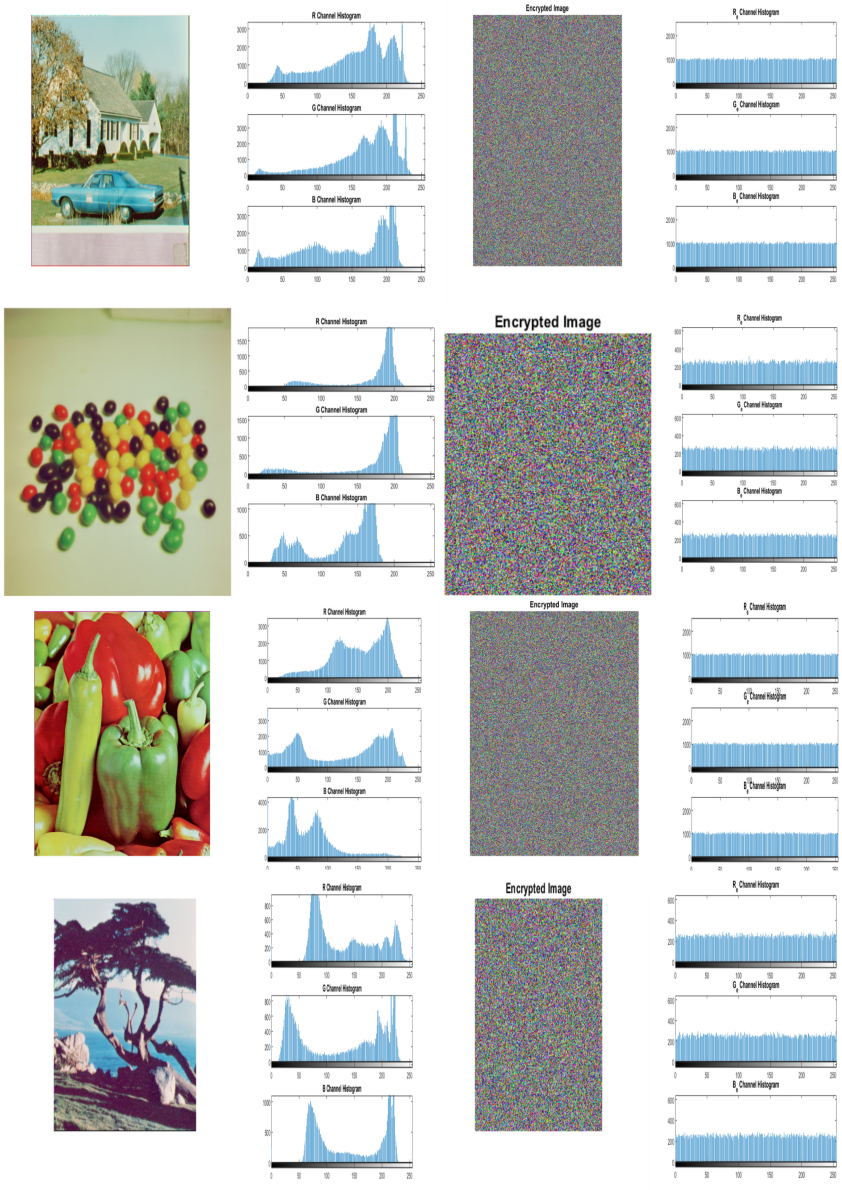


Fig. 6. Histograms of the images: (a) original images; (b) histogram of the original image; (c) encrypted image; (d) histogram of the encrypted image.

To ensure the encryption process operates correctly, the initial conditions and control parameters for the quantum logistic map are set.

$\upsilon = 0.9, \beta = 6, r = 3.99, r_1 = 0.05$

$x(1) = 0.05, y(1) = 0.02, z(1) = 0.05$

Step 4: Session keys are generated by the three-dimensional quantum logistic map.

The fractional-order quantum logistic map extends the classical logistic model by introducing a fractional derivative. At this stage, iterative processes are used to produce chaotic sequences. The system's dynamic solution, considering the fractional derivative, is formulated as follows:

$$x(i) = r.x(i-1)\cdot(1 - x(i-1) - r_1 \cdot y(i-1)$$

Step 5: Data padding.

A constant padding value is added to both ends of the vector to strengthen security during encryption. This step not only injects extra information into the process but also preserves the vector's original length.

$$padded - img - 1d = [padding - value: img - 1d' : padding - value]$$

Step 6: Key sequence generation.

The chaotic sequence generated by the quantum logistic map is converted into a key sequence for encryption through a mod 256 operation and integer conversion.

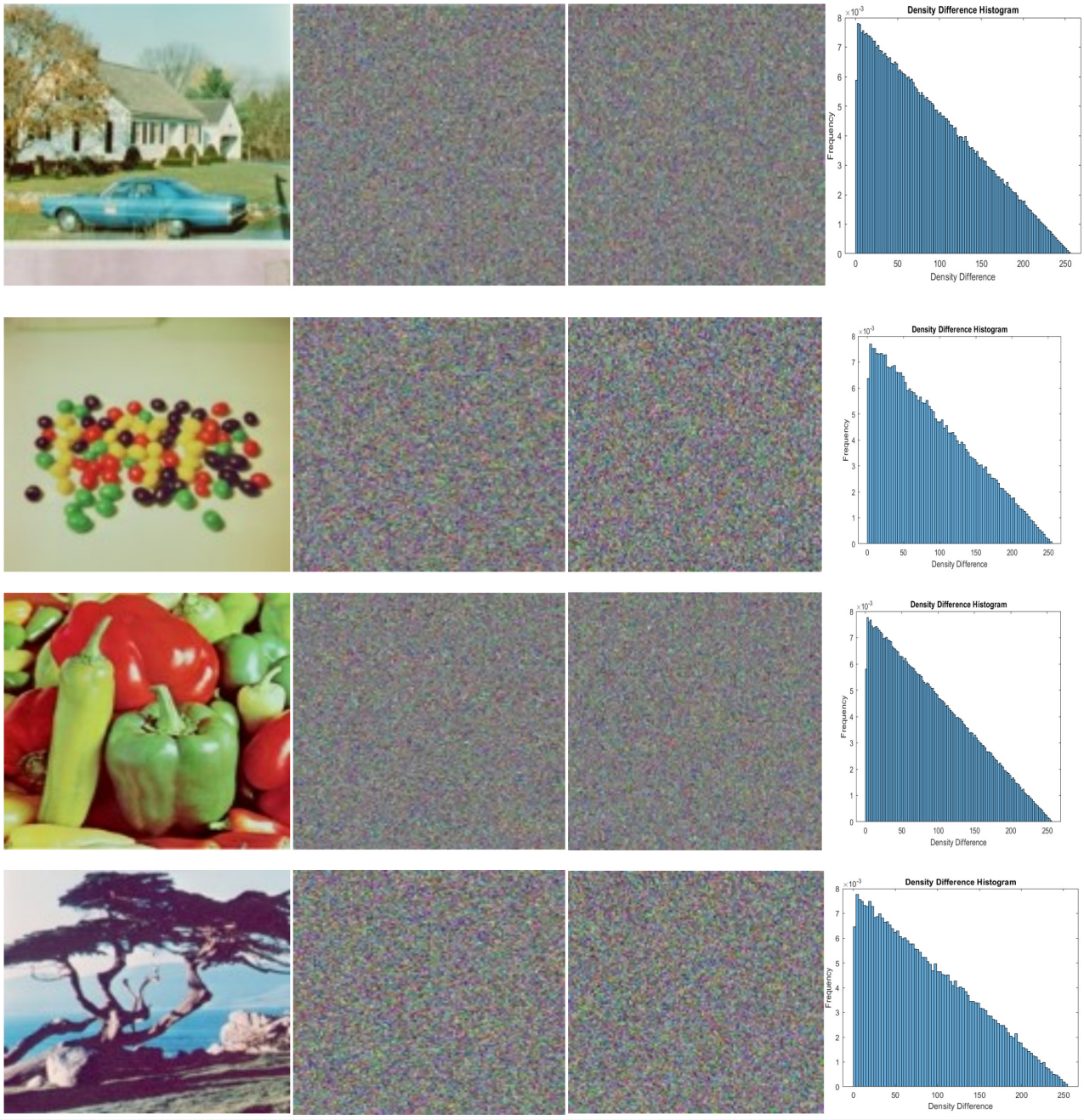


Fig. 7. Results of the encrypted images when the secret key is modified. (a) Original image; (b) Encrypted image with x(1) = 0.05 ; (c) Encrypted image with x(1) = 0.049; (d) Histogram plot of the intensity difference between the two encrypted images.

$xInt = uint8\ ((x \times 10^{15}) mod 256)$

Step 7: Encryption process.

The encryption process alters each pixel's value through the XOR operation. This technique not only hides data but also boosts security by promoting the diffusion of information. The first and last pixels are encrypted directly with XOR, while the intermediate pixels undergo an XOR operation involving both the previous encrypted pixel and the next one.

$encrypted\_image(I) = bitxor(bitxor(bitxor(M_{(m \times n \times p) \times 1}(I), xint(I)), encrypted\_image(I-1)), M_{(m \times n \times p) \times 1}(I+1)$

Step 8: Removal of padding and retrieval of the encryption image.

After the encryption process, the padding added to the beginning and end of the data vector is removed to restore the original data length.

Fig. 5 shows the block diagram of the quantum logistic map process with the steps given. The decryption is nearly identical to the

encryption with the reversed steps. As both encryption and decryption processes share a similar structure, they basically share the same time complexity and algorithmic complexity. The cipher image length is equal to the plain image. This feature is one of the most significant features of our presented cryptosystem.

D. Experimental results

1) National Institute of Standards and Technology Statistical Test Suite

The NIST statistical test suite was applied to assess the randomness of the proposed encryption algorithms. For a bit sequence to be considered random, the *P*-value obtained from each test must be greater than .01. Table I presents the NIST statistical test results for the encrypted "Banana" color image, with a size of 1000 × 1000.

2) Histogram Analysis

Histogram analysis visually represents the distribution of pixels in an image. To make the images more resistant to third-party attacks, the histograms of encrypted images are expected to exhibit a flat distribution. Fig. 6 shows both plain images and their histograms as well as encrypted images and their corresponding histograms. From the histogram plots of the encrypted images, it is evident that the proposed encryption scheme is vulnerable to statistical attacks.

3) Key Sensitivity Analysis

Key sensitivity analysis evaluates whether the proposed encryption scheme is sensitive to changes in the secret key. First, the image is encrypted using the secret key. Then, the secret key is slightly modified, and the image is encrypted again with the new key. The difference between the two encrypted images is expected to be substantial. To compare these images, a mathematical expression is used to calculate the ciphertext difference ratio (CDR). The pixels of the two encrypted images are XOR, and the number of '1's is divided by the total number of bits, with the result multiplied by 100. Fig. 7 shows the original and encrypted images and the histogram of the intensity difference. The CDR values are shown in Table II.

4) Information Entropy Analysis

Information entropy measures the irregularity and randomness in data [32]. High entropy values indicate strong security and high randomness in the encrypted image. The mathematical expression for calculating the information entropy is given in (5), as presented in [29]. $P(m_i)$, represents the probability of m_i and N denotes the number of intensity levels. Table III presents the entropy values for each channel of both the original and encrypted images.

TABLE II. DIFFERENT NUMBER OF BITS AND CIPHERTEXT DIFFERENCE RATIO VALUES BETWEEN THE ORIGINAL AND ENCRYPTED IMAGES

Image	Number of Different Bits	Total Number of Bits	CDR
House (512 × 512)	783.326	786.432	0.9961
Peppers (512 × 512)	783.374	786.432	0.9961
Tree (256 × 256)	195.821	196.608	0.9960
JellyBean (256 × 256)	195.860	196.608	0.9962

CDR, ciphertext difference ratio.

TABLE III. ENTROPY VALUES OF EACH CHANNEL IN THE ORIGINAL AND ENCRYPTED IMAGES

	Original Image			Encrypted Image		
Image	**R**	**G**	**B**	**R**	**G**	**B**
House	7.4157	7.2296	7.4355	7.9993	7.9993	7.9993
Peppers	7.3388	7.4963	7.0583	7.9993	7.9993	7.9992
Tree	7.2104	7.4136	6.9207	7.9975	7.9971	7.9975
JellyBean	5.7920	6.2195	6.7986	7.9970	7.9974	7.9974

$$H(m)=\sum_{i=0}^{2^N-1}P(m_i)\log_2\frac{1}{P(m_i)} \tag{5}$$

In Table IV, the entropy of plain image and cipher image is shown and compared with the results of [14, 26, and 23] for different images. As it can be inferred from the table, with the proposed algorithm, we obtain an entropy level very close to the theoretical maximum for 8 bits of a symbol. The proposed algorithm performs as well as other compared algorithms, as depicted in the table.

5) Correlation Analysis

The intrinsic properties of image data result in a strong correlation between adjacent pixels. To enhance resistance against attacks during transmission through insecure channels, minimizing the correlation between pixels is a key objective. The correlation coefficient is calculated as described in [32] using (6), where *N* represents the number of pixels and x_i and y_i denote the values of adjacent pixels.

$$r_{xy}=\frac{\sum_{i=1}^{N}\left(\left(x_i-E(x)\right)\left(y_i-E(y)\right)\right)}{\sqrt{\left(\sum_{i=1}^{N}\left(x_i-E(x)\right)^2\right)\left(\sum_{i=1}^{N}\left(y_i-E(y)\right)^2\right)}} \tag{6}$$

TABLE IV. COMPARATIVE ENTROPY VALUES WITH REFERENCE STUDIES [14], [26] AND [23]

Image	Channel	Entropy of Original Image	Entropy of Encrypted Image
House	R	7.4157	7.9993
	G	7.2296	7.9993
	B	7.4355	7.9993
[14]	–	–	7.9998
[26]	R	6.5724	7.9992
	G	7.4512	7.9992
	B	6.7626	7.9993
[23]	R	7.7066	7.9993
	G	7.4744	7.9994
	B	7.7522	7.9992

TABLE V. HORIZONTAL, VERTICAL AND DIAGONAL CORRELATIONS OF THE CHANNELS OF THE ORIGINAL AND ENCRYPTED IMAGES

		Original Image			Encrypted Image		
Image	**Colour**	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
House	R	0.9536	0.9579	0.9224	−0.0013	$-9.0624e-04$	$4.2679e-04$
	G	0.9391	0.9423	0.8901	0.0019	−0.0029	$2.9459e-04$
	B	0.9725	0.9686	0.9445	$5.8301e-04$	−0.0051	$5.6981e-04$
Peppers	R	0.9635	0.9663	0.9564	0.0013	0.0023	−0.0020
	G	0.9811	0.9818	0.9687	0.0014	−0.0051	0.0032
	B	0.9665	0.9664	0.9478	$-4.3769e-04$	−0.0050	$-4.7549e-04$
Tree	R	0.9590	0.9361	0.9159	0.0023	0.0071	−0.0038
	G	0.9687	0.9457	0.9318	$7.8491e-04$	−0.0042	$3.7105e-04$
	B	0.9612	0.9406	0.9265	−0.0084	0.0011	$-9.7164e-04$
JellyBean	R	0.9734	0.9741	0.9478	0.0063	− 0.0115	− 0.0061
	G	0.9708	0.9741	0.9470	$2.6146e-04$	−0.0038	−0.0079
	B	0.9779	0.9793	0.9583	−0.0045	0.0041	−0.0024

$$E(x)=\sum_{i=1}^{N}x_i \tag{7}$$

$$E(y)=\sum_{i=1}^{N}y_i \tag{8}$$

Table V presents the horizontal, vertical, and diagonal correlation coefficients of the original and encrypted color images. While the original images exhibit high correlation values between adjacent pixels, the encrypted images demonstrate significantly lower correlation values. This indicates that the proposed encryption algorithm effectively reduces the correlation between adjacent pixels. Fig. 8, 9, 10, and 11 illustrate the correlation distributions in all directions for the original and encrypted images "House," "Peppers," "Tree," and "Jellybean" which were selected from the database [27].

In Table VI, the correlation of the plain image and the cipher image is shown and compared with the results [14] and [26] for different images. As it can be inferred from the table with the proposed algorithm, the correlation, especially horizontal and diagonal correlations, outperforms the compared references, which is also an indication of good scrambling and confusion.

V. CONCLUSION

A quantum logistic map, known for its sensitivity to initial conditions, was selected for the secure storage and transmission of

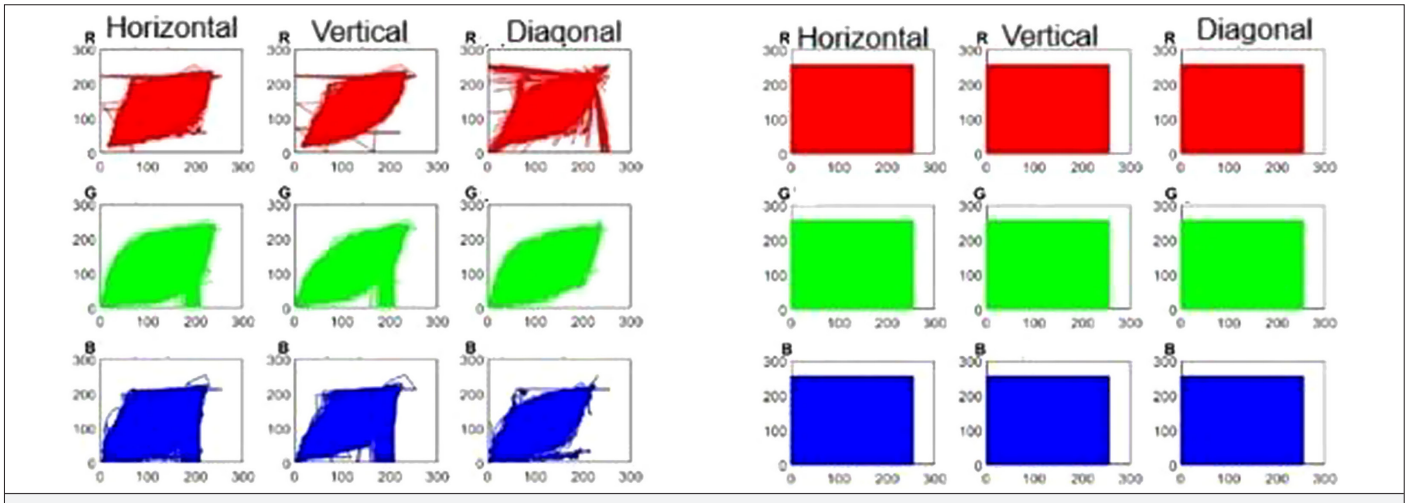


Fig. 8. Correlation distributions of the "House" image in all directions. (a) Correlation distribution of the original 'House' image in all directions; (b) Correlation distribution of the encrypted 'House' image in all directions.

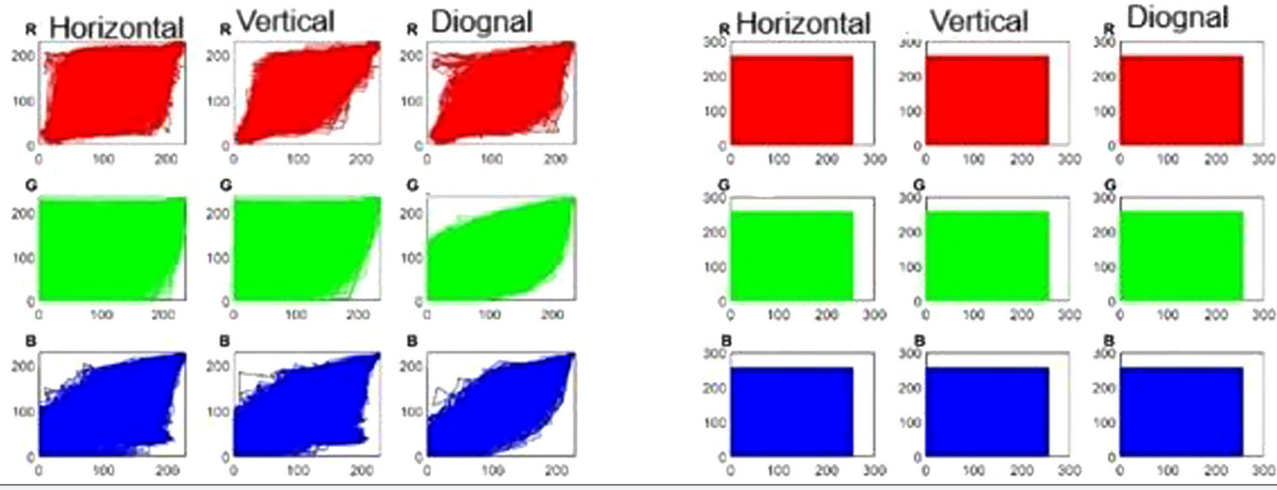


Fig. 9. Correlation distributions of the "Peppers" image in all directions. (a) Correlation distribution of the original "Peppers" image in all directions; (b) Correlation distribution of the encrypted "Peppers" image in all directions.

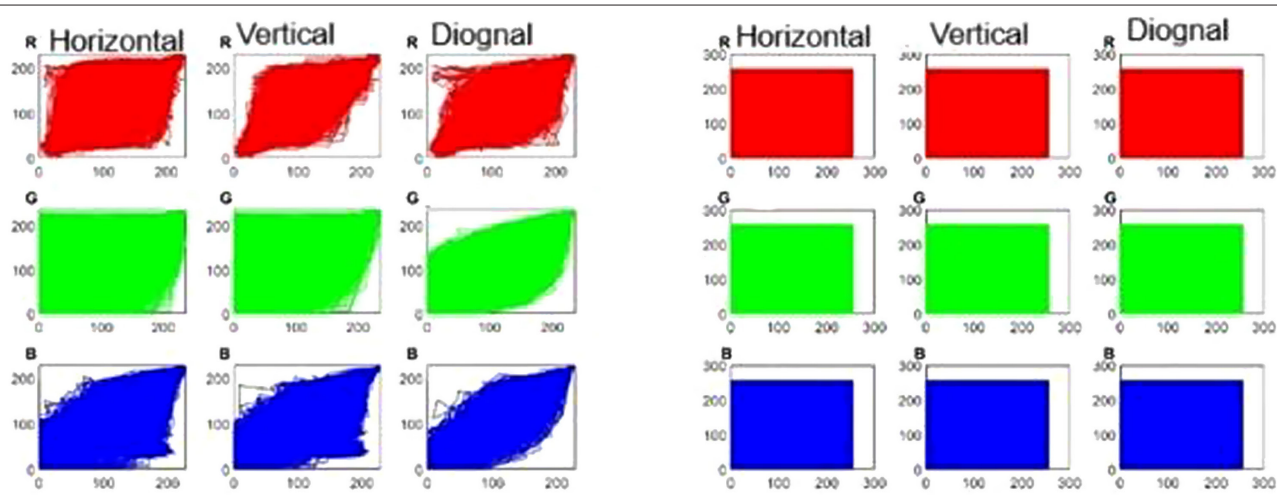


Fig. 10. Correlation distributions of the "Tree" image in all directions. (a) Correlation distribution of the original "Tree" image in all directions; (b) Correlation distribution of the encrypted "Tree" image in all directions.

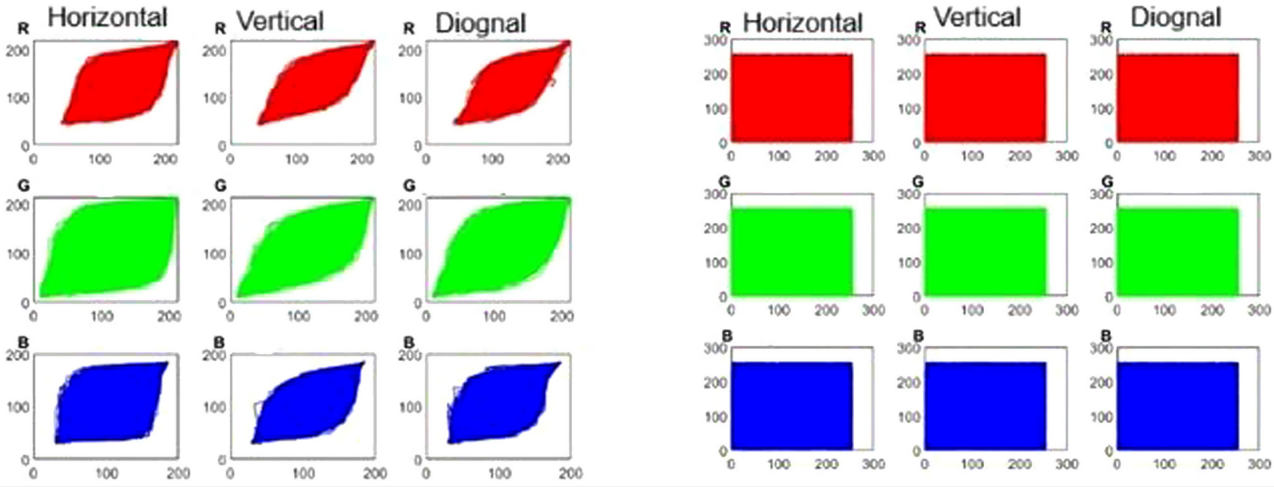


Fig. 11. Correlation distributions of the "JellyBean" image in all directions. (a) Correlation distribution of the original "JellyBean" image in all directions; (b) Correlation distribution of the encrypted "JellyBean" image in all directions.

TABLE VI. COMPARATIVE CORRELATION VALUES WITH REFERENCE STUDIES [14], [26]

Direction	[14] Plain Image	[14] Ciphered Image	[26] Plain Image R	[26] Ciphered Image R	[26] Plain Image G	[26] Ciphered Image G	[26] Plain Image B	[26] Ciphered Image B	House Plain Image R	House Ciphered Image R	House Plain Image G	House Ciphered Image G	House Plain Image B	House Ciphered Image B
Horizontal	0.9516	0.0065	0.9660	0.0092	0.9811	-0.0054	0.9661	0.0103	0.9536	-0.0013	0.9391	0.0019	0.9725	0.0006
Vertical	0.9447	0.0055	0.9656	0.0059	0.9822	0.0140	0.9669	0.0118	0.9579	-0.0009	0.9423	-0.0029	0.9686	-0.0051
Diagonal	0.9059	0.0082	0.9584	-0.0093	0.9630	0.0030	0.9489	0.0092	0.9224	0.0004	0.8901	0.0003	0.9445	0.0006

images over insecure channels. Color images were encrypted using the three-dimensional quantum logistic map, and performance analyses and experiments were conducted. The results of the NIST randomness test suite, histogram analysis, and entropy, and correlation analysis indicate successful randomness and, therefore successful confusion property of the proposed encryption schema. Moreover, key space analysis and CDR security analysis indicate a sufficiently secure space for the proposed algorithm. It can be concluded that the proposed algorithm demonstrates good performance in terms of encryption.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – M.C.K., M.K.; Design – M.C.K., M.K.; Supervision – M.C.K., M.K.; Resources – M.C.K., M.K.; Materials – M.C.K., M.K.; Data Collection and/or Processing – M.C.K., M.K.; Analysis and/or Interpretation – M.C.K., M.K.; Literature Search – M.C.K., M.K.; Writing – M.C.K., M.K.; Critical Review – M.C.K., M.K.

Declaration of Interests: The authors have no conflicts of interest to declare.

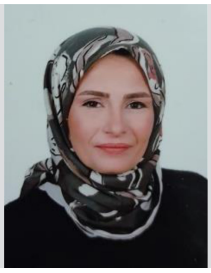
Funding: The authors declare that this study received no financial support.

REFERENCES

1. C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol.28, no. 4, pp. 656–715, Oct. 1949. [CrossRef]
2. E. N. Lorenz, *The Essence of Chaos*. Seattle, WA: University of Washington Press, 1993. [CrossRef]
3. S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos Solitons Fract.*, vol. 40, no. 5, pp. 2509–2519, 2009. [CrossRef]
4. M. Planck, "On the law of distribution of energy in the normal spectrum," *Ann. Phys.*, vol. 4, pp. 553–563, 1901. [CrossRef]
5. D. J. Griff, and D. F. Schroeter, *Introduction to Quantum Mechanics*, 3rd ed. Cambridge: Cambridge University Press, 2018.
6. A. Misra, "Quantum Superpositioning: Unraveling the mysteries of parallel realities," *ScienceOpen Preprints*, 2023. [CrossRef]
7. S. Aristarhov, "S. Heisenberg's uncertainty principle and particle trajectories," *Found. Phys.*, vol. 53, no. 1, 2023. [CrossRef]
8. W. H. Zurek, "Decoherence and the transition from quantum to classical," *Phys. Today*, vol. 44, no. 10, pp. 36–44, 1991. [CrossRef]
9. R. P. Feynman, R. B. Leighton, and M. Sands, *The Feynman Lectures on Physics, Vol. 3: Quantum Mechanics.* MA: Addison-Wesley, vol. 3, 1965.
10. S. S. Gill, A. Kumar, H. Singh et al., "Quantum computing: a taxonomy, systematic review and future directions," *Softw. Pract. Exper.*, vol. 52, no. 1, pp.66–114, 2022.
11. S. Basiri, L. F. M. Naseri et al., *"Quantum RGB Image Encryption based on Bit-planes and Logistic Map," PREPRINT (Version 1) available at Research Square. 2024 (https://doi.org/10.21203/rs.3.rs-3910283/v1)*[CrossRef]
12. R. Renner, and R. Wolf, "Quantum advantage in cryptography," *AIAA J.*, vol. 61, No. 5, pp. 1895–1910, 2023. [CrossRef]
13. C. M. Chandrashekar, S. Banerjee, and R. Srikanth, "Relationship between quantum walks and relativistic quantum mechanics," *Phys. Rev. A*, vol. 81, no. 6, p. 062340, 2010. [CrossRef]
14. A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, 2012. [CrossRef]
15. B. Xu, X. Ye, G. Wang, Z. Huang, and C. Zhang, "A fractional-order improved quantum logistic map: Chaos, 0–1 testing, complexity, and control," *Axioms*, vol.12, no. 1, p. 94, 2023. [CrossRef]
16. X. Liu, D. Xiao, and C. Liu, "Three-level quantum image encryption based on Arnold transform and logistic map," *Quantum Inf. Process.*, vol. 20, no. 1, 2021. [CrossRef].
17. X. Liu, D. Xiao, and Y. Xiang, "Quantum image encryption using intra and inter bit permutation based on logistic map," *IEEE Access*, vol. 7, pp. 6937–6946, 2019. [CrossRef]

18. Y. Dong, C. Yin, C. Xu, and R. Yan, "A quantum image encryption method for dual chaotic systems based on quantum logistic mapping," *Phys. Scr.*, vol. 99, no. 1, p. 015103, 2024. [CrossRef]
19. M. Brindha, and R. Vidhya, "A novel approach for chaotic image encryption based on block level permutation and bit –Wise substitution," *Multimedia Tool. Appl.*, vol. 81, pp. 3735–3772, 2021.
20. W. Song, C. Fu, Y. Zheng, M. Tie, J. Liu, and J. Chen, "A parallel image encryption algorithm using Intra bit plane scrambling," *Math. Comput. Simul.*, vol. 204, pp. 71–88, 2023. [CrossRef]
21. A. Bano, and P. Singh, "Image encryption using block-based transformation algorithm," *Pharm. Innov. J.*, vol. 8, pp. 11–18, 2019.
22. R.-G. Zhou, Q. Wu, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," *Int. J. Theor. Phys.*, vol. 52, no. 6, pp. 1802–1817, 2013. [CrossRef]
23. G. Ye, H. Wu, K. Jiao, and D. Mei, "Asymmetric image encryption scheme based on the quantum logistic map and cyclic module diffusion," *Math. Biosci. Eng.*, vol. 18, no. 5, pp. 5427–5448, 2021. [CrossRef]
24. E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with Sİmple logical functions," *Comput. Electr. Eng.*, vol.54, pp. 471–483, 2016. [CrossRef]
25. N. K.Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006. [CrossRef]
26. Y. Dong, X. Huang, Q. Mei, and Y. Gan, "Self-adaptive image encryption algorithm based on quantum logistic map," *Sec. Commun. Netw.*, vol. 2021, pp.1–12, 2021. [CrossRef]
27. *SIPI Image Database, University of Southern California Signal and Image Processing Institute* [Accessed: 29 May 2018].
28. R. B. Naik, and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Ann. Data. Sci.*, vol.11, no. 1, pp.25–50, 2024. [CrossRef]
29. E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Opt. Laser Technol.*, vol. 114, pp. 224–239, 2019. [CrossRef]
30. G. Ye, K. Jiao, X. Huang, B. M. Goi, and W. S. Yap, "An image encryption scheme based on public key cryptosystem and the quantum logistic map," *Sci. Rep.*, vol. 10, no. 1, 21044, 2020. [CrossRef]
31. M. E. Goggin, B. Sundaram, and P. W. Milonni, "Quantum logistic map," *Phys. Rev. A*, vol. 41, no. 10, pp. 5705–5708, 1990. [CrossRef]
32. C. Xu, "A novel color image encryption method using Fibonacci transformation and chaotic systems," *EAI Endorsed Scal Inf Syst.*, vol. 11, Jul. 2024. [CrossRef]

Mustafa Cem KASAPBAŞI works at Istanbul Commerce University, Computer Engineering Department of Engineering Faculty. His areas of expertise are steganography, chaos cryptography, data mining, management information systems, distance learning, and knowledge management.



Meryem KILIÇ works at Istanbul Commerce University, Computer Engineering Department of Engineering Faculty. She is currently pursuing her master's degree in computer engineering at the same university. Her research interests are chaotic encryption and data security.