Cluster Computing (2025) 28:3
https://doi.org/10.1007/s10586-024-04743-6

Quantum image encryption protocol for secure communication in healthcare networks

Sunil Prajapat[1] · Dheeraj Kumar[2] · Pankaj Kumar[1]

Received: 20 March 2024 / Revised: 12 August 2024 / Accepted: 17 August 2024 / Published online: 10 October 2024
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract
Maintaining patient confidentiality and ensuring data integrity are critical aspects of healthcare information security. In response to the growing need for enhanced security measures in the transmission and storage of medical images, the current study introduces a novel framework utilizing chaos-based quantum encryption. It enhances security in medical image transmission and storage. The proposed work presents a novel approach to quantum image encryption, integrating chaotic map and gray coding techniques. Specifically, it leverages quantum gray coding to obscure image data, followed by a quantum XOR operation using a key generated through the logistic-sin map for secure encryption. The encryption and decryption procedures leverage an NEQR quantum image representation. Simulations conducted in MATLAB assess the efficacy of the proposed image encryption protocol from both theoretical and statistical perspectives. The results demonstrate robust encryption performance, as evidenced by metrics such as an entropy value of 7.99, an UACI of 33.54%, an NPCR of 99.6%, and negative correlation coefficient values. The proposed scheme effectively decrypted tampered images, successfully recovering the maximum amount of information, as evidenced by tests with 50% data occlusion from encrypted images. These results emphasize the superior reliability, feasibility, and efficiency of the proposed quantum encryption protocol in securing medical image data during transmission and storage.

Keywords Quantum communication · Internet of Things (IoT) · Wireless communication · Image encryption

1 Introduction

In the modern era, fortifying the sanctity of digital image data has become an imperative, representing the forefront of technological integrity across multifaceted landscapes. This urgency is notably pronounced within the complex frameworks of military operations and healthcare systems [1–4]. Advanced encryption methodologies are essential for securing the transmission, storage, and retrieval of quantum images, particularly in critical applications such as medical imaging. Ensuring patient confidentiality requires encrypting user or patient data before transmission through IoT networks or communication channels [5–9]. Therefore, developing tailored methods for protecting medical quantum images is paramount for advancing applications within the healthcare industry.

A study [10] established two requirements that a well-designed healthcare image security solution should meet: confusion and diffusion. The term "confusion" refers to the cipher image's "indistinguishability" and the inability to separate it from the plain or secret image. Diffusion is the process via which significant alterations to the plain image or the key result in modifications to the cipher image. Many encryption techniques use the substitution box (S-box), a nonlinear component, to guarantee the confusion property [11]. Systems with chaotic dynamics can be used to verify the diffusion property. Indeed, a variety of ultimate characteristics of chaotic systems or maps, including ergodicity, sensitivity to initial conditions,

✉ Pankaj Kumar
pkumar240183@hpcu.ac.in

Sunil Prajapat
cuhp21rdmath13@hpcu.ac.in

Dheeraj Kumar
cuhp20rdcs01@hpcu.ac.in

[1] Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala 176 206, India

[2] School of Management, IMS Unison University, Dehradun 248009, India

and random behavior, can cause confusion and diffusion in the plain images to produce secure cipher images.

Quantum mechanics led to the development of quantum computing and, eventually, quantum computers to solve issues that are inefficiently solved by conventional computers. The concept of a quantum computer was first presented by Feynman in 1982. It is a unique processing paradigm that uses a physical machine that may accept input states as a superposition of numerous separate inputs in an output state [12–20]. Adequate representation models are used in quantum computers to collect and store images. Various representation models for quantum images are available in the literature, including "Multi-Channel representation of quantum image (MCRQI)" [21], Entangled Image [22], Real Ket [23], "Flexible representation of quantum images (FRQI)" [24], which uses $2m+1$ qubits to represent a $2^m \times 2^m$ gray image, and the "Novel enhanced quantum representation (NEQR)" [25], which uses $2m+p$ qubits to represent a $2^m \times 2^m$ gray image. Notwithstanding the fact that $(\mathcal{NEQR})$ requires more qubits $2m+p$ than FRQI, it is advantageous for quantum image processing since quantum color coding is highly comparable to classical image color coding.

Recent, active research projects worldwide focus on quantum technologies such as quantum teleportation, quantum cryptography, and quantum steganography, which may eventually result in more potent quantum computers. Patient safety and confidentiality are at stake when medical images from quantum healthcare systems are uploaded to the public cloud. Consequently, before transferring them to the cloud, they ought to be encrypted or shielded from harmful activity [26–32]. In recent years, there has been a notable surge in interest among scientists and technologists regarding quantum image encryption. A summary of several pioneering quantum image encryption techniques is provided below. Jiang et al. [33] demonstrated quantum scrambling techniques using Fibonacci and Arnold transformations, and also proposed a method based on the Hilbert scanning matrix. Additionally, Zhou et al. [34] introduced quantum scrambling approaches employing bit-plane and Gray coding. Yang et al. [35] presented a novel quantum image encryption technique involving double random-phase encoding and an extended Arnold transform. Similarly, Song et al. [36] devised a method utilizing constrained geometric transformations to rearrange pixel positions, followed by restricted color transformations for permutation. Moreover, Zhou et al. [34] proposed a quantum encryption technique that perturbs pixel coordinates using an Arnold transform and encodes color information via double random-phase operations.

To address the encapsulation of gray-level information, Gong et al. [37] proposed a technique based on quantum *XOR* (exclusive OR) operations derived from chaotic systems. Additionally, Liang et al. [38] introduced a quantum technique utilizing *XOR* operations with the logistic map to encrypt gray-level information. Furthermore, numerous studies have emerged focusing on enhancing the security of healthcare media and its associated technologies.

Quantum image processing is advancing rapidly in the realm of quantum computing and can be effectively executed on the Noisy Intermediate-Scale Quantum (NISQ) device [39, 40]. Quantum image encryption plays a crucial role in this field. Nevertheless, the encryption process frequently faces security flaws and involves intricate computational intricacies, resulting in the consumption of significant quantum resources [41–44]. In order to tackle this issue, this paper introduces a robust, chaotic quantum encryption scheme designed specifically for securing medical image data. Moreover, the scheme is founded upon a chaotic logistic-sin map and gray code, ensuring heightened security measures. Medical personnel access the images from the cloud subsequent to their transmission by healthcare staff. By employing the appropriate decryption keys, staff members can securely assist patients in deciphering the encrypted data embedded within the images. The encryption process begins with the utilization of quantum gray-code to scramble the quantum image. Subsequently, *XOR* operations, facilitated by a key generator managed by the logistic-sine map, are employed to encrypt the jumbled quantum image. In the proposed medical cryptosystem, the medical images are divided into two distinct parts: one containing the high 4 bits of each image and the other containing the low 4 bits. To bolster security measures, the hash value for the split images is obtained using the $SHA-256$ hashing algorithm. This modernizes the initial conditions of quantum gates and the logistic map, thereby ensuring plain image sensitivity within the proposed medical cryptosystem. Notably, as the high 4 bits image encompasses a significant amount of information (94.125% of the total data), it is encrypted using quantum techniques, while the other image, containing a relatively small amount of information (only 5.875% of the total data), is encrypted using a logistic map. Simulation studies affirm the efficiency, feasibility, and reliability of the proposed quantum image encryption method compared to its classical counterpart. Moreover, the method proves to be swift and well-suited for secure imaging in medical systems. The subsequent sections delineate the key contributions of this work in detail.

- A robust chaotic quantum encryption scheme is presented for securing medical image data to utilize a chaotic logistic-sin map and gray code.
- Medical cryptosystems demonstrate high sensitivity to even the slightest alterations in the original images.

– The high 4 bits image, encompassing 94.125% of the complete medical information, undergoes encryption employing a quantum model.
– Experimental results validate the proposed medical encryption scheme's robust security to demonstrate resilience against various attacks.

1.1 Paper organization

The paper follows this structure: Sect. 2 introduces the quantum preliminaries, covering essential definitions and fundamentals of quantum theory. Section 3 delves into the specific construction of the quantum encryption scheme designed for healthcare data. Subsequently, Sect. 4 outlines the simulation results derived from the proposed approach and comparison with state-of-the-art. Finally, Sect. 5 concludes the paper.

2 Quantum preliminaries

2.1 Novel enhanced quantum representation ($\mathcal{NEQR}$)

The 2×2 ($\mathcal{NEQR}$) image model employs quantum principles to encode a 2×2 grid of pixels, ensuring enhanced security through quantum randomness and non-equilibrium states. This model utilizes quantum properties to generate and manipulate pixel values, resulting in a compact yet highly secure representation of digital images. Each discrete pixel within an image is characterized by a unique combination of color and spatial coordinates, both of which are encompassed within the $\mathcal{NEQR}$ [25, 45] model. In a quantum scenario, an image of size $2^m \times 2^m$ is mathematically represented as follows:

$$|\mathcal{I}\rangle = \frac{1}{2^m} \sum_{j=0}^{4^m-1} |\alpha_j\rangle \otimes |j\rangle \tag{1}$$

Here in, $\otimes$ represents tensor product of $|\alpha_j\rangle, |j\rangle$.

Where,

$$|\alpha_j\rangle = |\alpha_j^{p-1}, \ldots \alpha_j^1, \alpha_j^0\rangle, \quad \alpha_j^k \in \{0,1\},$$
$$j = 0, 1, \ldots, 4^m - 1,$$
$$k = 0, 1, \ldots, p-1.$$

The colour value and colour range 2^p, $|j\rangle$ for $j = 0, 1, \ldots, 4^m - 1$ with 4^m dimension computational basis is encoded by the sequence $\alpha_j^{p-1}, \ldots \alpha_j^1, \alpha_j^0$. The ($\mathcal{NEQR}$) encapsulates information pertaining to colors and their respective spatial coordinates within the image, partitioned into two distinct segments for encoding, $|\alpha\rangle_j$ and $|j\rangle$, respectively.

$$\begin{aligned} |\mathcal{I}\rangle &= \frac{1}{2}(|0\rangle \otimes |00\rangle + |56\rangle \otimes |01\rangle \\ &\quad + |128\rangle \otimes |10\rangle + |255\rangle \otimes |11\rangle) \\ &= \frac{1}{2}(|00000000\rangle \otimes |00\rangle + |00111000\rangle \otimes |01\rangle \\ &\quad + |10000000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle) \end{aligned}$$

2.2 Gray code

A prominent technique utilized for signal coding in digital conversions is the Gray code. The mathematical formula defining the Gray code is as follows:

$$\mathcal{G}_j = \mathcal{T}_j \oplus \mathcal{T}_{j+1}, \quad j = o, 1, \ldots, p-1$$
$$\mathcal{G}_p = \mathcal{T}_p$$

where $\mathcal{T}$ is a positive integer with the binary code $(\mathcal{T}_p \mathcal{T}_{p-1} \ldots \mathcal{T}_1 \mathcal{T}_0)$. An example of reflected Gray and binary codes is displayed in Fig. 1.

2.3 Bit plane

A bit plane refers to the collection of bits representing each pixel value within an image at a specific bit position. For instance, pixel values in an image typically range from 0 to 255, represented in binary form as 8-bit data. The most significant digit (MSD) bit plane decomposition represents each pixel value in an image in binary format. The bit planes correspond to the binary digits (bits) of these pixel values, ranging from the most significant bit (MSB) Fig. 2's eighth image (8) to the least significant bit (LSB) in Fig. 2's first image (1). The most significant bit plane

No.	Binary Code				Gray Code			
0	0	0	0	1	0	0	0	1
1	0	0	1	0	0	0	1	1
2	0	0	1	1	0	0	1	0
3	0	1	0	0	0	1	1	0
4	0	1	0	1	0	1	1	1
5	0	1	1	0	0	1	0	1
6	0	1	1	1	0	1	0	0
7	1	0	0	0	1	1	0	0
8	1	0	0	1	1	1	0	1
9	1	0	1	0	1	1	1	1
10	1	0	1	1	1	1	1	0
11	1	1	0	0	1	0	1	0
12	1	1	0	1	1	0	1	1
13	1	1	1	0	1	0	0	1
14	1	1	1	1	1	0	0	0
15								

Fig. 1 An illustration showcasing reflected Gray and binary codes

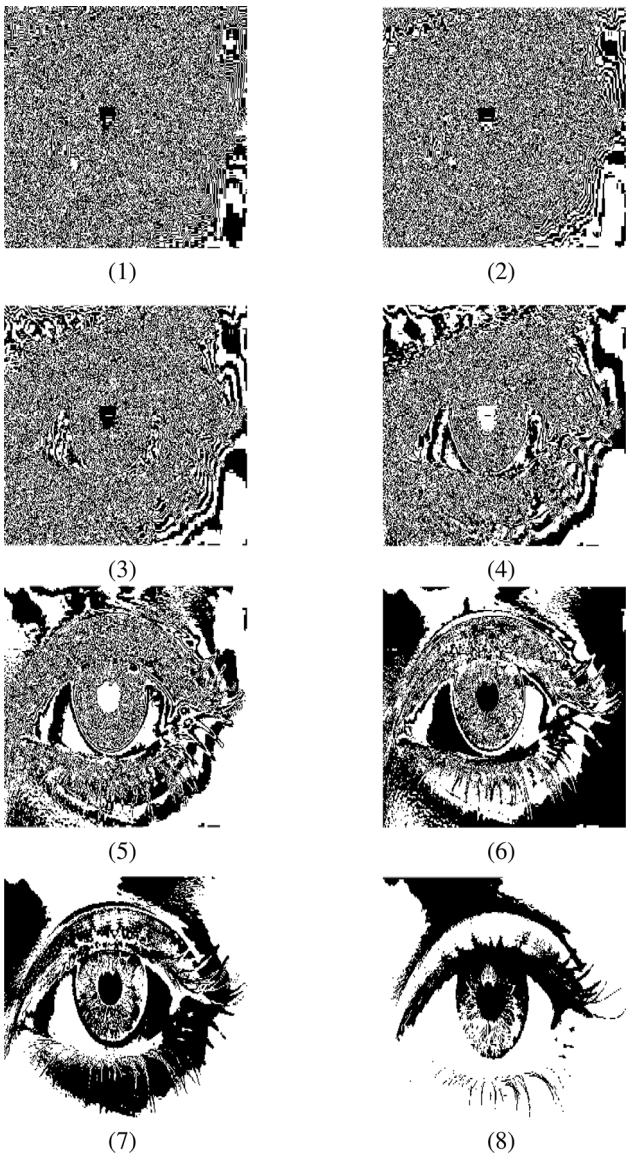

Fig. 2 Variation of eye image bit-planes from 1 to 8

contains the most prominent information, while the least significant bit plane contains the least significant information. Figure 2 demonstrates an example of bit planes for an eye image.

2.4 Controlled-not ($\mathcal{CNOT}$) operation

The $\mathcal{CNOT}$ gate, which features two inputs—the control qubit and the target qubit, serves as the quantum analog of the classical *XOR* gate. When the control qubit is in the state $|1\rangle$, the gate flips the state of the target qubit; conversely, if the control qubit is in the state $|0\rangle$, the gate remains inactive. By employing the secret key as the control qubit, encryption of the quantum image represented by the target qubit can be achieved. The gate is represented by a unitary matrix.

$$\mathcal{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

2.5 The chaotic map

The one-dimensional discrete chaotic map, termed the logistic-*sin* map [46, 47], is formulated as follows:

$$k_{j+1} = \varphi(k_j - k_j^2) + (4 - \varphi)\sin\frac{(\pi k_j)}{4} (\text{mod } 1) \tag{3}$$

where k_0 is the starting value and φ is the control parameter, which $\varphi \in [0, 4]$. The bifurcation, which displays the strong attractor in the chosen map, is seen in Fig. 3.

2.6 System model

The illustrated framework delineating the secure encryption of healthcare data is depicted in Fig. 4. In this scheme, pivotal medical images undergo encryption utilizing the proposed quantum encryption system, administered collaboratively by users and medical professionals situated at a singular location. Following encryption, the ciphered images are transmitted to cloud storage. Medical professionals stationed remotely retrieve these encrypted images from the cloud and engage our proposed decryption technique to unveil the underlying data. Through the deployment of our quantum encryption scheme, users and other pertinent system stakeholders can be unequivocally assured of the absolute confidentiality of the transmitted healthcare data.

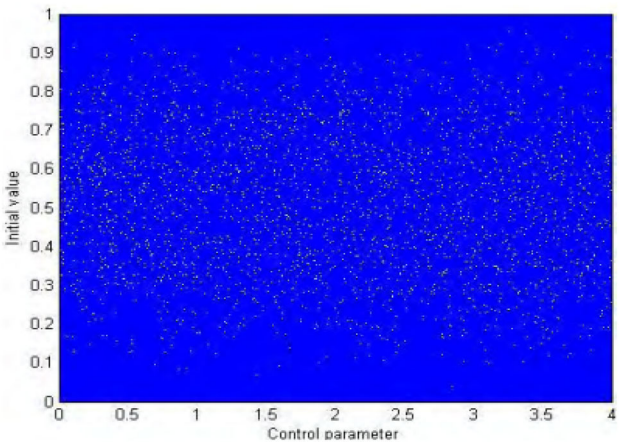

Fig. 3 Bifurcation on the map

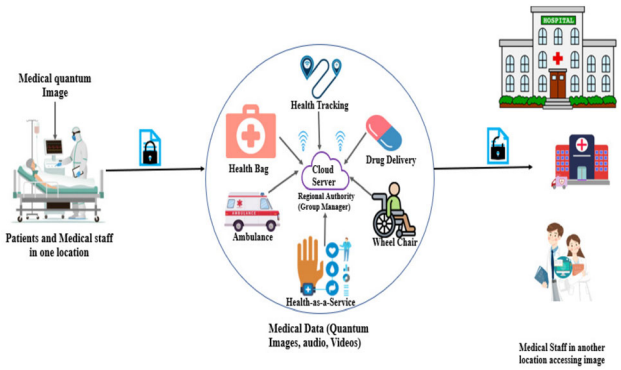

Fig. 4 System model: framework overview

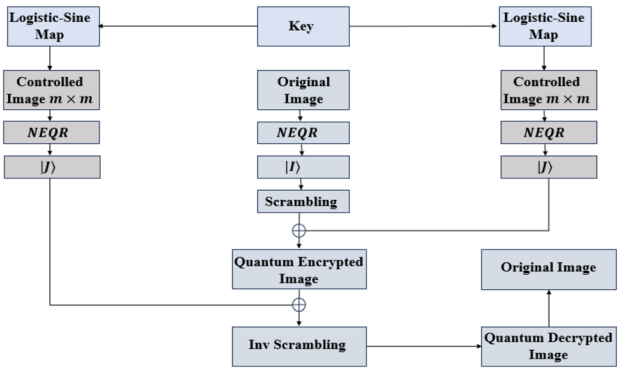

Fig. 5 Flow diagram of the proposed scheme

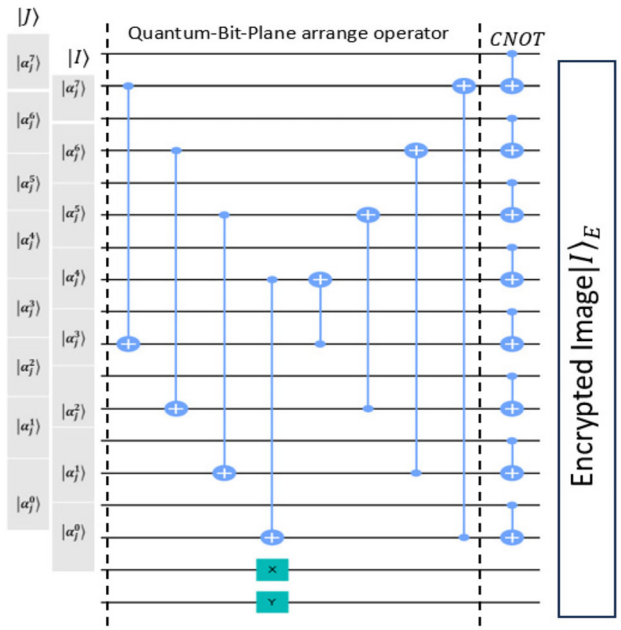

Fig. 6 Quantum Circuit diagram of the encryption process

3 Concrete construction of quantum encryption scheme for healthcare data

The innovative quantum encryption method for brain-computer interface images relies on quantum controlled-not gates, quantum bit-plane structure Gray coding, and quantum images represented by $\mathcal{NEQR}$. Figure 5 illustrates the proposed quantum encryption algorithm, while the circuit for it is displayed in Fig. 6.

3.1 Encryption process

The encryption process of the proposed scheme involves three procedures, detailed in Algorithm 1 as follows:

1. Evolution of quantum image,
2. Transformation of sequences, and
3. Encryption of quantum image.

As shown in Fig. 6, the quantum image $|\mathcal{I}\rangle$ is encrypted by modifying the $\mathcal{CNOT}$ operations on the scrambled image $|\mathcal{I}\rangle_s$.

Algorithm 1 Encryption Procedure

Input: Medical data (Images), Set of secret keys k_j, φ_j.
Output: Encrypted quantum image $|\mathcal{I}_E\rangle$.

procedure EVOLUTION QUANTUM IMAGE($\mathcal{CNOT}$)
  Randomly choose secret keys k_j, φ, where $k_0 \in (0,1)$ and $\varphi_0 \in [0,4]$.
  Keys are used in map $k_{j+1} = \varphi(k_j - k_j^2) + (4-\varphi)\sin\frac{(\pi k_j)}{4} \pmod 1$. Where $j = 0, 1, ..., 4^m$, (4^m is the size of image).
end procedure
procedure TRANSFORMS OF SEQUENCES($\{k_j \rightarrow$ Integer$\}$)
  Choose a sequence $k_j^* = |fix\,[(K_j - fix\,(K_j)) \times 10^8]| \pmod{256}$
  Apply $\mathcal{NEQR}$ to transform the k_j^* sequence into a quantum image representation. $|\mathcal{J}\rangle = \frac{1}{2^n}\sum_{i=0}^{4^n}|\alpha\rangle_i \otimes |i\rangle$, $|\alpha_i\rangle = |\alpha_i^8, ...\alpha_i^0\rangle, \alpha_i^k \in (0,1)$
  Convert the original medical image to a quantum $|\mathcal{I}\rangle = \frac{1}{2^n}\sum_{j=0}^{4^n}|\alpha\rangle_j \otimes |j\rangle$, $|\alpha_i\rangle = |\alpha_i^8, ...\alpha_i^0\rangle, \alpha_i^k \in (0,1)$
end procedure
procedure ENCRYPTION OF QUANTUM IMAGE($|\mathcal{I}_E\rangle$)
  Utilizes the quantum bit plane and gray code for scrambling.
  Scrambling of quantum image $|\mathcal{I}\rangle$
  Encryption the Scrambled quantum image $|\mathcal{I}\rangle_s$
  return $|\mathcal{I}\rangle_E$
end procedure

3.2 Decryption process

During the encryption process, the first two parameters, denoted as k_j and φ, serve as the encryption keys. As outlined in Algorithm 2, the decryption procedure operates inversely to the encryption process, effectively unraveling

the encrypted data. Figure 7 illustrates the quantum circuit diagram of the decryption process.

Algorithm 2 Decryption Procedure

Input: : Encrypted quantum image, k_j, φ.
Output: Result Valid (1) or Invalid (0).

procedure EVOLUTION QUANTUM IMAGE($\mathcal{CNOT}$)
  Set values of secret keys k_j, φ, to obtain quantum image $|\mathcal{I}\rangle$.
end procedure
procedure $\mathcal{CNOT}$ PROCESS()
  By applying $\mathcal{CNOT}$ operation on ciphered quantum image $|\mathcal{I}\rangle_E$
  Obtain scrambling quantum image $|\mathcal{I}\rangle$.
end procedure
procedure DESCRAMBLING QUANTUM IMAGE($|\mathcal{I}_E\rangle$)
  $|\mathcal{I}_s\rangle$ is descrambled using quantum bit plane and gray code.
  if Outcome valid. **then**
    return 1
  end if
  if Outcome invalid. **then**
    return 0
  end if
end procedure

4 Simulation results

A series of simulation analyses were conducted on a personal computer featuring an Intel Core i7 processor operating at 2.80 GHz and equipped with 16 GB of RAM to validate the proposed algorithm. The encryption of images was performed using MATLAB R2021b, with the image dimensions set to 256×256. The outcomes of the experiments are depicted in Fig. 8, illustrating both the original and encrypted images.

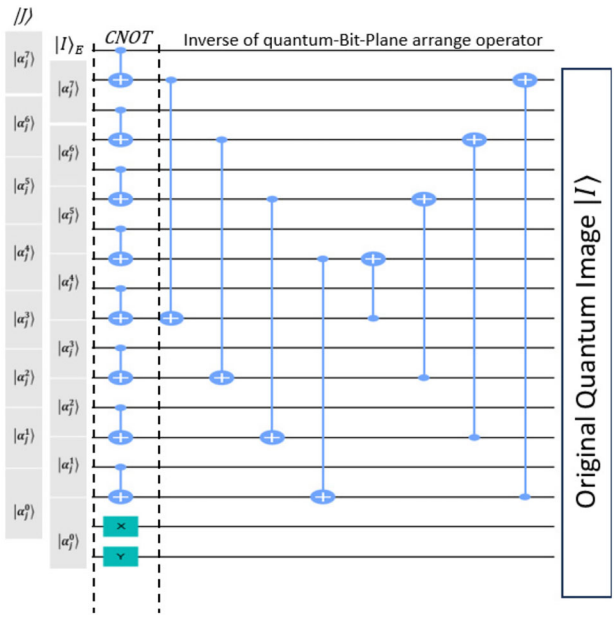

Fig. 7 Quantum circuit diagram of the decryption process

Several tests and various security analysis techniques are employed in these sections to evaluate the robustness of the proposed algorithm.

4.1 Key space analysis

The security of the encryption algorithm is heavily dependent on the size of the key. Attempting a brute-force attack against a sufficiently large key poses a formidable challenge. Encryption employing large key sizes creates substantial obstacles for brute-force attacks. In this method, a 1656-bit standard quantum qubit is employed, resulting in a key space of 2^{1656}. Table 1 illustrates how the proposed scheme's key space is incredibly vast when compared to other schemes. It is consequently more resistant to a brute-force attack.

4.2 Key sensitivity analysis

Key sensitivity pertains to the characteristic wherein minor alterations in the secret key induce substantial modifications in the cipher image. Encrypting various images using a single, immutable secret key enables the evaluation of key sensitivity. For decryption, substantially modified keys are employed. Incorrect keys fail to decrypt the plain image. Encrypted images, when decrypted using an incorrect key even if it varies slightly from the secret key must not divulge any information about the confidential data and should exhibit complete dissimilarity. Hence, the key sensitivity exhibited by this method is deemed appropriate.

4.3 Correlation analysis

A robust image encryption scheme is essential to eliminate the significant correlation present among pixels within an image. Correlation coefficients were utilized to analyze the correlation between pixels. The correlation coefficient representing the relationship between pixel x and pixel y is denoted as follows:

$$r = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{1}{n} \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\frac{1}{n}\sum (x_i - \bar{x})^2 \cdot \frac{1}{n}\sum (y_i - \bar{y})^2}}$$

where r is the correlation coefficient, x_i and y_i are the individual data points, $\bar{x}$ and $\bar{y}$ are the means of the x and y variables, respectively.

An effective encryption method necessitates the correlation value to be substantially close to zero for the cipher image. Table 2 and Fig. 9 illustrate the correlation coefficient results in each neighboring direction for two pixels of both the plain images and the cipher images. As the correlation between neighboring pixels tends towards zero, the

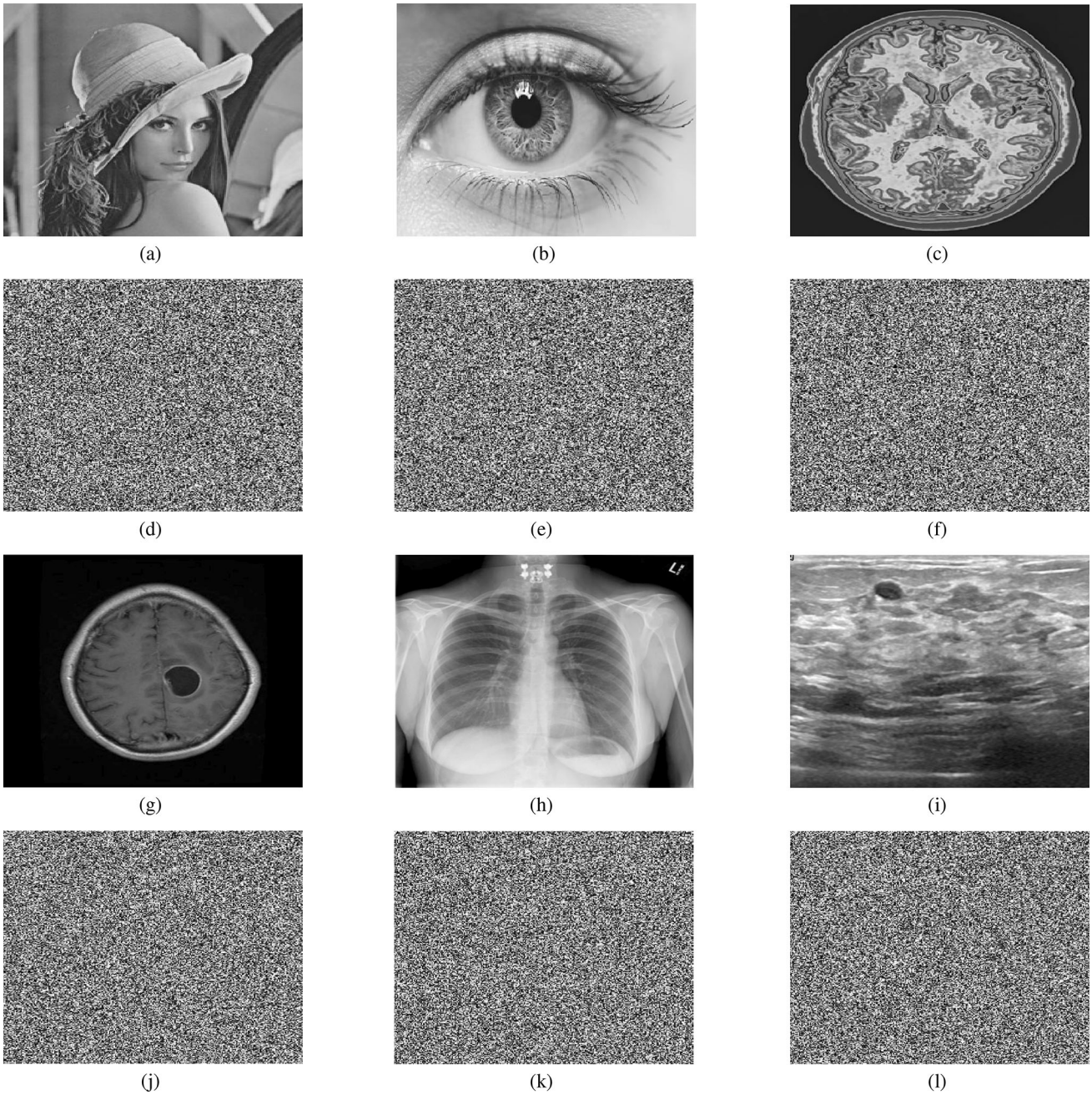

Fig. 8 **a** Lena, **b** Human Eye, **c** Human Brain, **d** Cipher Image of Lena, **e** Cipher Image of Human Eye, **f** Cipher Image of Human Brain, **g** MRI image, **h** Xray image, **i** Ultrasound image, **j** Cipher Image of MRI, **k** Cipher Image of Xray, **l** Cipher Image of Ultrasound

dissimilarity between them increases, rendering it more challenging for an attacker to infer the pixel values of other pixels based on the relationship between nearby pixels. Given that our results exhibit values remarkably close to zero, the attacker is unable to exploit the pixel relationships to discern information about the plain image.

4.4 Histogram analysis

The histogram illustrates the distribution of pixel intensity within the image. Typically, attackers exploit discernible patterns within the histograms of plain images to extract information using statistical techniques. A robust encryption technique should yield a uniform histogram for the cipher image [58]. Hence, eliminating inter-pixel correlation and ensuring a uniform distribution of pixels in the encrypted image are imperative. Histograms of several

Table 1 Comparison of key spaces

References	Key space
[48]	$\approx 9.017 \times 10^{14}$
[49]	$2^{701} - 2^{500}$
[50]	2^{255}
[51]	10^{56}
[52]	2^{256}
[53]	$4^{256\times256}$
[54]	2^{112}
[55]	–
[56]	2^{656}
[57]	–
Proposed	2^{1656}

Table 2 Resultant correlation analysis of adjacent pixels

Images	Vertical	Diagonal	Horizontal
Figure 8a	0.9754	0.9648	0.9761
Figure 8d	− 0.0089	− 0.0018	− 0.0021
Figure 8b	0.9176	0.8937	0.9796
Figure 8e	− 0.0079	− 0.0108	− 0.0035
Figure 8c	0.9588	0.9377	0.9689
Figure 8f	− 0.0204	0.0096	− 0.149
Figure 8g	0.9674	0.9784	0.9186
Figure 8h	− 0.0078	− 0.0019	− 0.0018
Figure 8i	0.9331	0.9137	0.8996
Figure 8j	− 0.0074	− 0.0210	− 0.0031
Figure 8k	0.9588	0.9932	0.9689
Figure 8l	− 0.0196	0.0096	− 0.149

plain images and their associated encrypted counterparts are depicted in Fig. 10. To validate the efficacy of the proposed approach, we conducted a histogram analysis to ascertain the uniform distribution of pixels. It is crucial that the histograms of encrypted images exhibit uniform distribution to adequately represent the original data. For instance, the simulated brain image, the eye photograph, and the Lena image, all sized 256×256, display uniform histograms. Therefore, based on the histogram analysis, the proposed methodology performs admirably as evidenced by the uniformity observed in both the encrypted images and their histograms.

4.5 Information entropy analysis

The degree of randomness in pixel values is measured by entropy. An 8-bit image's entropy is described as.

$$H(m) = -\sum_{i=0}^{255} P(x_i) \times \log P(x_i)$$

where $P(x_i)$ is the probability of x_i, x_i is the gray value equivalent to pixel value i.

An effective encryption technique yields a cipher image with an entropy value approaching 8 bits. Table 3 presents the entropy values before and after encryption. The encrypted images exhibit entropies close to 8 bits, signifying the resilience of the proposed encryption method against entropy attacks. Hence, the performance of our algorithm is deemed satisfactory.

4.6 Number of pixel change rate and unified average changing intensity analysis

The influence of altered pixels in the original image on the encrypted image is assessed through two methodologies: the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). NPCR quantifies the rate of alteration between the pixels of the original image and the encrypted counterpart. UACI evaluates the disparity between the original and encrypted images. The formula is as follows:

$$NPCR = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} P(i,j) \times 100\%$$

$$UACI = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{C_1(i,j) - C_2(i,j)}{255} \times 100\%$$

$$P(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

where $m \times n$ is the size of the image, $C_1(i,j)$ is the cipher image before a pixel change, $C_2(i,j)$ is the modified cipher image after a pixel change, $P(i, j)$ is the bipolar network.

As shown in Table 4, the average UACI and NPCR values across all images are 33.46 and 99.61%, respectively. This indicates that the encryption scheme's key demonstrates high sensitivity, as a significant modification in the key results in substantial alterations in most pixels of the cipher image. The elevated NPCR and UACI values signify the robustness of our method against differential attacks. Consequently, our proposed approach exhibits a high level of sensitivity to minor pixel modifications within images.

4.7 Comparative analysis

The proposed scheme will be subjected to comparative analysis with relevant existing methodologies. Security parameters including key space, variance, correlation coefficient, entropy, *UACI*, and *NPCR* will be scrutinized. Comparative tests demonstrate that the proposed scheme has the lowest variance and correlation coefficient,

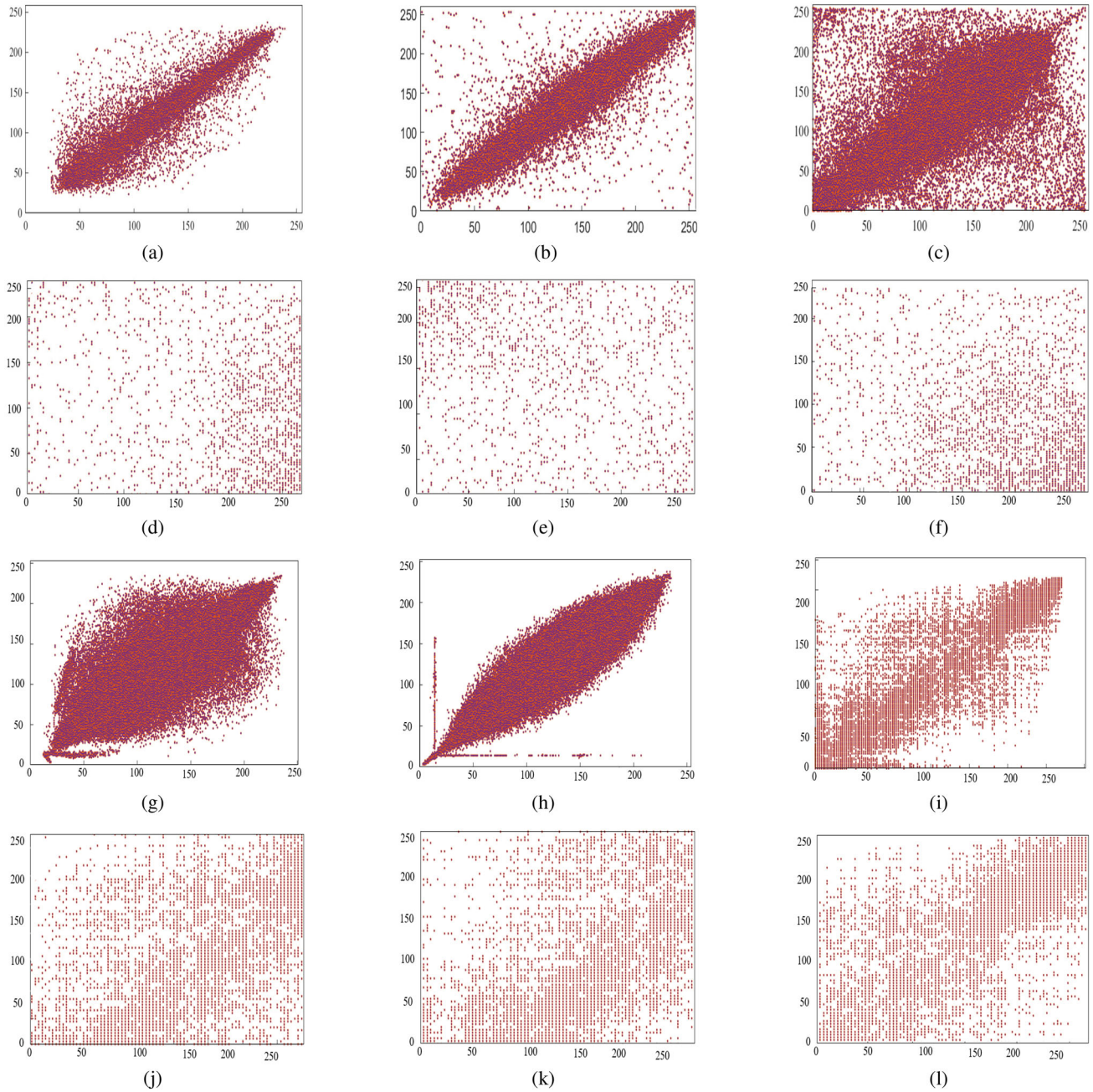

Fig. 9 Correlation analysis of adjacent pixels in plain and encrypted images

the highest entropy, *UACI*, and *NPCR* values, as well as the largest key space, the simplest computations, and the best encryption technique, as shown in Table 5. These findings affirm the robustness and efficacy of the proposed approach.

4.8 Resistance attack analysis

There are typically four types of attacks: ciphertext-only attack, known plaintext attack, chosen plaintext attack, and chosen ciphertext attack [61]. Chosen-plaintext attacks are more powerful than others because they allow the attacker to choose a plaintext and obtain its corresponding ciphertext. If the proposed algorithm is resistant to chosen-plaintext attacks, it can also withstand other types of attacks. The starting keys k_j, φ are randomly chosen, and the keys are used to map the images into the quantum images associated with the plaintext, which are then retrieved by the quantum measurement. Thus, the attacker is unable to compromise the cryptosystem through the process of encrypting and decrypting selected plaintext

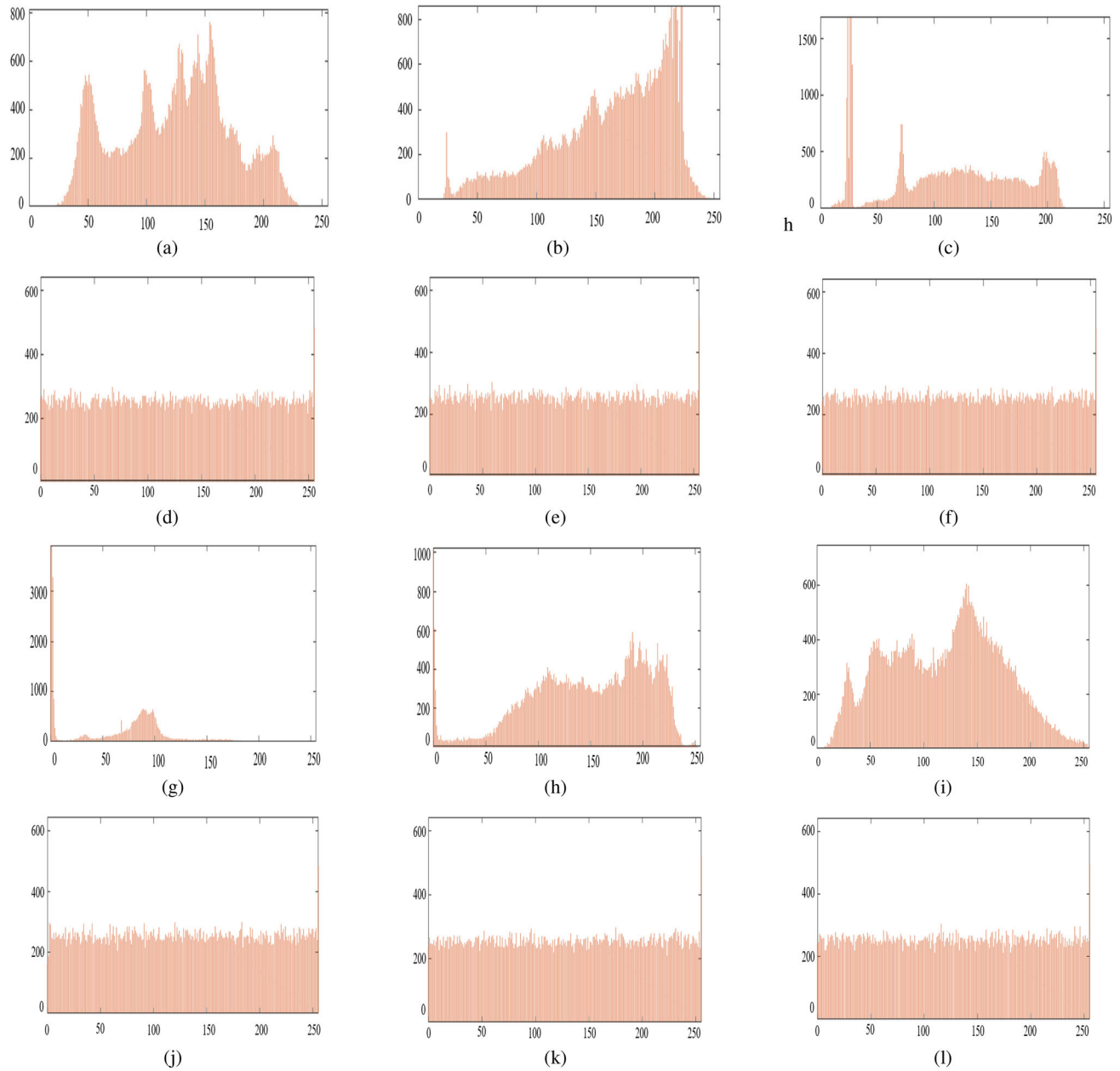

Fig. 10 Histograms of adjacent pixels of plain and encrypted images

Table 3 Entropy analysis: assessment of information entropy

Images	Plain image	Encrypted image
Figure 8a (99.60%)	7.1246	7.9888
Figure 8b (99.53%)	6.9863	7.9899
Figure 8c (99.60%)	6.3249	7.9896
Figure 8g (99.55%)	7.3246	7.6999
Figure 8h (99.56%)	7.9863	6.9899
Figure 8i (99.60%)	7.3249	7.7526

images. The proposed scheme is resistant to chosen-plaintext attacks and other types of attacks.

4.9 Occlusion attacks

The transmission of digital images over networks raises considerable issues related to noise and data loss, which can severely undermine the integrity of an encrypted image. A major concern in this context is occlusion attacks, commonly known as data loss attacks. These attacks involve a calculated effort by an adversary to remove particular elements from a ciphered image, thereby

Table 4 NPCR and UACI tests

	0.05-Level	0.01-Level	0.001-Level
Theoretical NPCR	99.5996%	99.5664 %	99.5496 %
Figure 8a (99.60%)	✓	✓	✓
Figure 8b (99.53%)	✓	✓	✓
Figure 8c (99.60%)	✓	✓	✓
Figure 8g (99.55%)	✓	✓	✓
Figure 8h (99.56%)	✓	✓	✓
Figure 8i (99.60%)	✓	✓	✓
Theoretical UACI	33.4992%	33.1782%	33.0632%
Figure 8a (33.46%)	✓	✓	✓
Figure 8b (33.49%)	✓	✓	✓
Figure 8c (33.53%)	✓	✓	✓
Figure 8g (33.50%)	✓	✓	✓
Figure 8h (33.49%)	✓	✓	✓
Figure 8i (33.51%)	✓	✓	✓

✓: Pass, ×: Fail

hindering or obstructing the decryption process. To determine the percentage of occlusion present in an image, the following formula is utilized:

$$\%\text{Occlusion} = \frac{\text{Area of Occluded Region}}{\text{Total Area of the Image}} \times 100$$

The proposed technique has been evaluated in the context of both data loss attacks and noise attacks. The findings demonstrate that, despite a 50% decrease in the size of the encrypted images, the algorithm successfully decrypted the image and retained the maximum amount of information.

4.10 Computational complexity analysis

In order to attain both concurrency and consistency, the computational complexity of executing different processes is assessed based on CPU operations. The encryption method presented consists of four phases: picture splitting, key generation, permutation, and substitution. The process of separating the two plain-medical images involves a

Table 5 Comparison with state-of-art

References	Key space	Variance	Correlation coefficient	Entropy	*UACI*	*NPCR*	Complexity	Encryption technique
[48]	$\approx 9.017 \times 10^{14}$	–	0.0023	–	–	–	–	Arnold scrambling, wavelet transforms
[49]	$2^{701} - 2^{500}$	–	− 0.0013	7.9967	27.31	99.58	–	One-particle quantum walks
[50]	2^{255}	–	0.0351	–	–	–	$o(n2^{n+1})$	Phase-shift transform, Quantum haar wavelet packet transform
[51]	10^{56}	–	− 0.0013	–	–	–	$o(n)$	*XOR* operations
[52]	2^{256}	239.48	− 0.0800	–	–	–	$o(n2^n)$	Neural Adaptive Switching System
[53]	$4^{256\times256}$	–	0.0019	7.9970	33.17	99.60	$o(2^{2n})$	DNA-CNOT
[54]	2^{112}	285.64	0.001	7.9971	–	–	–	Feistel structure
[55]	–	240.64 – 0.00465	− 0.0201	7.9972	–	99.65	$o(n^2)$	Scrambling for G-NEQR
[56]	2^{656}	240.64	− 0.00465	7.9974	33.51	99.62	–	Self-adaptive hash function-controlled chaotic map
[57]	–	243.69	− 0.0219	7.9970	33.52	99.53	$o(2^n)$	Bit-plane permutation and sine logistic map
[59]	2^{128}	240.33	− 0.0221	7.9990	33.44	99.61	$o(2^2)$	Four-dimensional Lorenz system
[60]	2^{232}	243.33	− 0.0421	7.9890	33.44	99.61	$o(2^2)$	Two-dimensional triangle function combined with a discrete chaotic map
Proposed	2^{1656}	238.30	− 0.00460	7.9975	33.54	99.60	$O(\max(xy\log xy, n^2))$	Bit-plane permutation, sine logistic map, Quantum fundamentals CNOT

spatial complexity of $O(xy)$, where xy indicates the dimensions of the plain image. The key generation method involves iterating the logistic map xy times and executing quantum $\mathcal{CNOT}$. The spatial complexity for these processes are $O(xy)$ and $O(n^2)$, respectively. Sorting processes and calculating the index of each component are employed at the permutation stage, utilizing computational cost are. $O(xy\log(xy))$. The substitution phase employs the bit wise *XOR* operation, with a spatial complexity of $O(xy)$. The computational complexity of the encryption system is determined by the spatial complexity of each phase. It can be expressed as $O(\max(xy\log xy, n^2))$.

When assessing the effectiveness of an image cryptosystem, it is crucial to take into account the encryption time required for an image. This component plays a critical role in determining the effectiveness of the cryptosystem. To assess the cryptographic system's efficiency, we calculate the encryption time (measured in Mbits per second) of the proposed encryption scheme. The decryption procedure in the proposed cryptosystem is identical to the encryption process speed 5.4746 Mbit/s, but in reverse order and without executing the hashing method. Hence, the time required for deciphering is less than the time required for ciphering. Specifically, the proposed approach has a deciphering speed of 13.8735 Mbit/s. The results show that the proposed cryptosystem is appropriate for medical systems that require real-time processing.

5 Conclusion

In conclusion, this study presents a novel quantum image encryption scheme designed specifically for securing medical data. The proposed scheme leverages the principles of chaotic logistics and classical quantum mechanics. It involves converting patient images into an NEQR representation onsite, followed by encryption using a novel methodology before transmission to cloud storage. Through comprehensive testing and evaluation, the study demonstrates the efficacy and resilience of the proposed approach to protecting the confidentiality of medical data. More specifically, the results of our study reveal strong encryption performance, as indicated by various metrics: an entropy value of 7.99, UACI of 33.54%, NPCR of 99.6%, and negative correlation coefficient values. These findings highlight the effectiveness, practicality, and efficiency of the proposed quantum encryption protocol in securing medical image data during both transmission and storage.

Future endeavors aim to advance this groundwork by developing an advanced medical cryptosystem incorporating shared secret mechanisms, thereby further enhancing the security of medical data transmission and storage by employing blockchain technology.

Author contributions "Sunil Prajapat: Conceptualization, software, validation, writing, visualization. Dheeraj Kumar: Conceptualization, validation, reviewing and editing, data curation. Pankaj Kumar: Conceptualization, validation, reviewing and editing, investigation."

Funding No funding has been received for this paper.

Data availability Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Loan, N.A., Parah, S.A., Sheikh, J.A., Akhoon, J.A., Bhat, G.M.: Hiding electronic patient record (EPR) in medical images: a high capacity and computationally efficient technique for e-healthcare applications. J. Biomed. Inform. **73**, 125–136 (2017)
2. Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., Rayappan, J.B.B.: Medical data sheet in safe havens-a tri-layer cryptic solution. Comput. Biol. Med. **62**, 264–276 (2015)
3. Cao, F., Huang, H.K., Zhou, X.Q.: Medical image security in a HIPAA mandated PACS environment. Comput. Med. Imaging Graph. **27**(2–3), 185–196 (2003)
4. Shamim Hossain, M., Muhammad, G.: Cloud-assisted speech and face recognition framework for health monitoring. Mob. Netw. Appl. **20**, 391–399 (2015)
5. Shamim Hossain, M., Muhammad, G., Mizanur, S.M., Rahman, W.A., Alelaiwi, A., Alamri, A.: Toward end-to-end biomet rics-based security for IoT infrastructure. IEEE Wirel. Commun. **23**(5), 44–51 (2016)
6. Alluhaidan, A.S., Prabu, P.: End to end encryption in resource-constrained IoI device. IEEE Access (2023)
7. Alexan, W., Korayem, Y., Gabr, M., El-Aasser, M., Maher, E.A., El-Damak, D., Aboshousha, A.: Anteater: when Arnold's cat meets Langton's ant to encrypt images. IEEE Access **11**, 106249–106276 (2023)
8. Gabr, M., Korayem, Y., Chen, Y.-L., Yee, P.L., Chin Soon, K., Alexan, W.: R3-rescale, rotate, and randomize: a novel image cryptosystem utilizing chaotic and hyper-chaotic systems. IEEE Access **11**, 119284–119312 (2023)
9. Alexan, W., El-Damak, D., Gabr, M.: Image encryption based on Fourier-DNA coding for hyperchaotic Chen system, Chen-based binary quantization s-box, and variable-base modulo operation. IEEE Access **12**, 21092–21113 (2024)
10. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
11. Alemami, Y., Mohamed, M.A., Atiewi, S., Mamat, M.: Speech encryption by multiple chaotic maps with fast Fourier transform. Int. J. Electr. Comput. Eng. (IJECE) **10**(6), 5658–5664 (2020)
12. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2010)
13. Lo, H.-K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)

14. Gupta, R., Singh, R., Gehlot, A., Akram, S.V., Yadav, N., Brajpuriya, R., Yadav, A., Yongling, W., Zheng, H., Biswas, A., et al.: Silicon photonics interfaced with microelectronics for integrated photonic quantum technologies: a new era in advanced quantum computers and quantum communications? Nanoscale **15**(10), 4682–4693 (2023)
15. Ali, R.S., Akif, O.Z., Jassim, S.A., Farhan, A.K., El-Kenawy, E.-S.M., Ibrahim, A., Ghoneim, M.E., Abdelhamid, A.A.: Enhancement of the cast block algorithm based on novel s-box for image encryption. Sensors **22**(21), 8527 (2022)
16. Farhan, A.K., Al-Saidi, N.M.G., Maolood, A.T., Nazarimehr, F., Hussain, I.: Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder. Entropy **21**(10), 958 (2019)
17. Farhan, A.K., Ali, R.S., Natiq, H., Al-Saidi, N.M.G.: A new s-box generation algorithm based on multistability behavior of a plasma perturbation model. IEEE Access **7**, 124914–124924 (2019)
18. Zahid, A.H., Ahmad, M., Alkhayyat, A., Hassan, M.T., Manzoor, A., Farhan, A.K., et al.: Efficient dynamic s-box generation using linear trigonometric transformation for security applications. IEEE Access **9**, 98460–98475 (2021)
19. Farhan, A.K., Ali, R.S., Rashed Yassein, H., Al-Saidi, N.M.G., Abdul-Majeed, G.H.: A new approach to generate multi s-boxes based on RNA computing. Int. J. Innov. Comput. Inf. Control **16**(1), 331–348 (2020)
20. Kanwal, S., Inam, S., Ali, R., Cheikhrouhou, O., Koubaa, A.: Lightweight noncommutative key exchange protocol for IoT environments. Front. Environ. Sci. **10**, 996296 (2022)
21. Sun, B., Le, P.Q., Iliyasu, A.M., Yan, F., Garcia, J.A., Dong, F., Hirota, K.: A multi-channel representation for images on quantum computers using the rgbα color space. In 2011 IEEE 7th International Symposium on Intelligent Signal Processing, pp. 1–6. IEEE (2011)
22. Venegas-Andraca, S.E., Ball, J.L.: Processing images in entangled quantum systems. Quantum Inf. Process. **9**(1), 1–11 (2010)
23. Latorre, J.I.: Image compression and entanglement. arXiv preprint arXiv:quant-ph/0510031 (2005)
24. Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process. **10**, 63–84 (2011)
25. Zhang, Y., Kai, L., Gao, Y., Wang, M.: Neqr: a novel enhanced quantum representation of digital images. Quantum Inf. Process. **12**, 2833–2860 (2013)
26. Singh, A.K., Swain, S.R., Saxena, D., Lee, C.-N.: A bio-inspired virtual machine placement toward sustainable cloud resource management. IEEE Syst. J. (2023)
27. Azad, Y., Kumar, A.: Ethics and artificial intelligence: a theoretical framework for ethical decision making in the digital era. In: Digital Technologies, Ethics, and Decentralization in the Digital Era, pp. 228–268. IGI Global (2024)
28. Prajapat, S., Kumar, P., Kumar, S., Das, A.K., Shetty, S., Hossain, M.S.: Designing high-performance identity-based quantum signature protocol with strong security. IEEE Access (2024)
29. Prajapat, S., Kumar, P., Kumar, S.: A privacy preserving quantum authentication scheme for secure data sharing in wireless body area networks. Clust. Comput. 1–17 (2024)
30. Prajapat, S., Rana, A., Kumar, P., Das, A.K.: Quantum safe lightweight encryption scheme for secure data sharing in internet of nano things. Comput. Electr. Eng. **117**, 109253 (2024)
31. Kumari, D., Kumar, P., Prajapat, S.: A blockchain assisted public auditing scheme for cloud-based digital twin healthcare services. Clust. Comput. **27**(3), 2593–2609 (2024)
32. Thakur, G., Prajapat, S., Kumar, P., Das, A.K., Shetty, S.: An efficient lightweight provably secure authentication protocol for patient monitoring using wireless medical sensor networks. IEEE Access (2023)
33. Jiang, N., Wen-Ya, W., Wang, L.: The quantum realization of Arnold and Fibonacci image scrambling. Quantum Inf. Process. **13**(5), 1223–1236 (2014)
34. Zhou, R.-G., Sun, Y.-J., Fan, P.: Quantum image gray-code and bit-plane scrambling. Quantum Inf. Process. **14**, 1717–1734 (2015)
35. Yang, Y.-G., Xia, J., Jia, X., Zhang, H.: Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Inf. Process. **12**, 3477–3493 (2013)
36. Song, X.-H., Wang, S., Abd, A.A., El-Latif, Niu, X.-M.: Quantum image encryption based on restricted geometric and color transformations. Quantum Inf. Process. **13**, 1765–1787 (2014)
37. Gong, C.: Chaotic adaptive fireworks algorithm. In Advances in Swarm Intelligence: 7th International Conference, ICSI 2016, Bali, Indonesia, June 25–30, 2016, Proceedings, Part I 7, pp. 515–525. Springer, Berlin (2016)
38. Liang, H.-R., Tao, X.-Y., Zhou, N.-R.: Quantum image encryption based on generalized affine transform and logistic map. Quantum Inf. Process. **15**, 2701–2724 (2016)
39. Kanwal, S., Inam, S., Cheikhrouhou, O., Mahnoor, K., Zaguia, A., Hamam, H.: Analytic study of a novel color image encryption method based on the chaos system and color codes. Complexity **2021**(1), 5499538 (2021)
40. Kanwal, S., Inam, S., Hajjej, F., Cheikhrouhou, O., Nawaz, Z., Waqar, A., Khan, M.: A new image encryption technique based on sine map, chaotic tent map, and circulant matrices. Secur. Commun. Netw. **2022**(1), 4152683 (2022)
41. Inam, S., Kanwal, S., Zahid, A., Abid, M.: A novel public key cryptosystem and digital signatures. Eur. J. Eng. Sci. Technol. **3**(1), 22–30 (2020)
42. Inam, S., Kanwal, S., Firdous, R., Hajjej, F.: Blockchain based medical image encryption using Arnold's cat map in a cloud environment. Sci. Rep. **14**(1), 5678 (2024)
43. Inam, S., Kanwal, S., Ali, R.: A new encryption scheme based on groupring. Contemp. Math. 103–112 (2021)
44. Prajapat, S., Gautam, D., Kumar, P., Jangirala, S., Das, A.K., Park, Y., Lorenz, P.: Secure lattice-based aggregate signature scheme for vehicular ad hoc networks. IEEE Trans. Veh. Technol. (2024)
45. Wang, H., Tan, J., Huang, Y., Zheng, W.: Quantum image compression with autoencoders based on parameterized quantum circuits. Quantum Inf. Process. **23**(2), 41 (2024)
46. Dhingra, D., Dua, M.: Medical video encryption using novel 2d cosine-sine map and dynamic DNA coding. Med. Biol. Eng. Comput. 1–19 (2023)
47. Hua, Z., Zhou, Y., Pun, C.-M., Philip Chen, C.L.: 2d sine logistic modulation map for image encryption. Inf. Sci. **297**, 80–94 (2015)
48. Wen-Wen, H., Zhou, R.-G., Luo, J., Jiang, S.-X., Luo, G.-F.: Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. Quantum Inf. Process. **19**, 1–29 (2020)
49. Abd-El-Atty, B., El-Latif, A.A., Venegas-Andraca, S.E.: An encryption protocol for NEQR images based on one-particle quantum walks on a circle. Quantum Inf. Process. **18**(9), 272 (2019)
50. Li, H.-S., Li, C.Y., Chen, X., Xia, H.Y.: Quantum image encryption based on phase-shift transform and quantum Haar wavelet packet transform. Mod. Phys. Lett. A **34**(26), 1950214 (2019)
51. Gong, L.-H., He, X.-T., Cheng, S., Hua, T.-X., Zhou, N.-R.: Quantum image encryption algorithm based on quantum image XOR operations. Int. J. Theor. Phys. **55**, 3234–3250 (2016)

52. Li, H.-S., Li, C., Chen, X., Xia, H.: Quantum image encryption algorithm based on NASS. Int. J. Theor. Phys. **57**, 3745–3760 (2018)
53. Zhou, S.: A quantum image encryption method based on DNACNot. IEEE Access **8**, 178336–178344 (2020)
54. Guo, L., Hongwei, D., Huang, D.: A quantum image encryption algorithm based on the Feistel structure. Quantum Inf. Process. **21**, 1–18 (2022)
55. Li, H.-S., Chen, X., Song, S., Liao, Z., Fang, J.: A block-based quantum image scrambling for GNEQR. IEEE Access **7**, 138233–138243 (2019)
56. Abdelfatah, R.I.: Quantum image encryption using a self-adaptive hash function-controlled chaotic map (SAHF-CCM). IEEE Access **10**, 107152–107169 (2022)
57. Liu, X., Xiao, D., Liu, C.: Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. Quantum Inf. Process. **19**, 1–23 (2020)
58. Murugadoss, B., Karna, S.N.R., Kode, J.S., Subramani, R.: Blind digital image watermarking using Henon chaotic map and elliptic curve cryptography in discrete wavelets with singular value decomposition. In: 2021 International Symposium of Asian Control Association on Intelligent Robotics and Industrial Automation (IRIA), pp. 203–208. IEEE (2021)
59. Liu, X.-D., Chen, Q.-H., Zhao, R.-S., Liu, G.-Z., Guan, S., Liang-Long, W., Fan, X.-K.: Quantum image encryption algorithm based on four-dimensional chaos. Front. Phys. **12**, 1230294 (2024)
60. Patel, S., Thanikaiselvan, V., Rearajan, A.: Secured quantum image communication using new two dimensional chaotic map based encryption methods. Int. J. Theor. Phys. **63**(2), 49 (2024)
61. Liu, X., Xiao, D., Huang, W., Liu, C.: Quantum block image encryption based on Arnold transform and sine chaotification model. IEEE Access **7**, 57188–57199 (2019)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Sunil Prajapat received the M.Sc. degree in mathematics from the Central University of Himachal Pradesh, Dharamshala, India, in 2021, where he is currently pursuing the Ph.D. degree with the Srinivasa Ramanujan Department of Mathematics. His research interests are quantum cryptography, post-quantum cryptography, coding theory, Blockchain, and various applications of cryptographic primitives in the real world. He is a renowned Reviewer for numerous IEEE, Taylor and Francis, MDPI, PLOS One, Elsevier, and Springer journals. Mr. Prajapat is a CSIR Fellow.

Dheeraj Kumar received the Junior Research Fellowship (JRF) award letter from the University Grant Commission, India, in 2020. He is currently working toward the doctoral degree in computer science and Information Technology with Central University of Himachal Pradesh Dharamshala, India. His current research interests include IoT, fog computing, cloud computing, and Quantum computing

Pankaj Kumar received his M.Sc. from CCS University Meerut India and Ph.D. degrees from Galgotias University in 2005 and 2020, respectively. He has been an assistant professor at Srinivasa Ramanujan Department of Mathematics in the Central University of Himachal Pradesh, Dharamshala H.P. He has published over 40 academic research papers on information security and privacy preservation. His current research interests include Cryptography, Blockchain, Wireless Network Security, Information Theory, and Network Coding.