Journal of Modern Optics

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tmop20

QMedShield: a novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud

Arun Amaithi Rajan & Vetriselvi Vetrian

JOURNAL OF MODERN OPTICS
https://doi.org/10.1080/09500340.2024.2436521

Taylor & Francis
Taylor & Francis Group

QMedShield: a novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud

Arun Amaithi Rajan and Vetriselvi Vetrian

Security Research Lab, Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai, Tamil Nadu, India

ABSTRACT

In the age of digital technology, medical images play an important role in the healthcare industry, which aids surgeons in making precise decisions and reducing the diagnosis time. However, the storage of large amounts of these images in third-party cloud services raises privacy and security concerns. There are a lot of classical security mechanisms to protect them. Although, the advent of quantum computing entails the development of quantum-based encryption models for healthcare. There is a significant demand for resource-efficient, quantum-secure image encryption mechanisms that leverage existing classical infrastructure. Hence, in this paper, a novel quantum chaos-based encryption scheme for medical images has been introduced. The model utilizes bit-plane scrambling, a 3D quantum logistic map, quantum operations in the diffusion phase, a hybrid chaotic map, and DNA encoding in the confusion phase to transform the plain medical image into a cipher medical image. The proposed scheme has been evaluated using multiple statistical analyses and validated against more attacks such as differential attacks, known and chosen plaintext attacks with three different medical datasets, and theoretically, as well. Hence, the introduced encryption model has proved to be more attack-resistant and robust than other existing image encryption schemes, ensuring the secure storage of medical images in cloud environments.

ARTICLE HISTORY
Received 25 July 2024
Accepted 22 November 2024

KEYWORDS
Medical images; secure storage; quantum computing; quantum chaotic map; DNA encoding

1. Introduction

In the contemporary landscape, digital images serve as important tools across several domains, facilitating communication, documentation, analysis, and creative expression. Recent statistics indicate that 1.81 trillion pictures are captured yearly, which is anticipated to rise by 10–14% each year just from mobile phones. By 2030, experts predict that we might have 30 trillion images [1]. From the numbers, It is evident that images play a significant role in conveying information and enhancing understanding.

In the domain of healthcare, images have become indispensable nowadays. Medical images contain more intricate and important information about the patient. By using advanced imaging technologies, internal structures and abnormalities can be visualized by healthcare professionals, and the progression of diseases can be identified with more clarity and precision. They help physicians make timely decisions. These sensitive medical images need to be protected with image encryption strategies. The encryption methods used during transmission and those used for cloud storage differ in a few ways. While the objective of both types of encryption is to protect data, encryption for transmission protects data while it is in motion [2], and encryption for storage protects data while it is at rest in a persistent storage environment. As these highly sensitive medical images increase exponentially and are stored in third-party cloud servers, which are prone to cyber-attacks [3]. Even minor modifications to those medical images lead to erroneous diagnoses [4]. So, this article focuses more on secure storage solutions for medical images. Given the prime importance of security and privacy in medical image storage, it is imperative that all medical information be securely stored, with the responsibility for implementing necessary measures resting on the information owners. This can be achieved through medical image encryption techniques, which ensure the security of the medical image in cloud storage. The general process of storing medical images securely is illustrated in Figure 1.

In the insecure cloud, encrypting images emerges as the most efficient and secure technique for their storage. There exist various classical image encryption techniques. Kaur et al. [5] categorized them and discussed each method's pros and cons. Most image encryp-

CONTACT Arun Amaithi Rajan ✉ arunamaithirajan@gmail.com 🖃 Security Research Lab, Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai, Tamil Nadu 600025, India

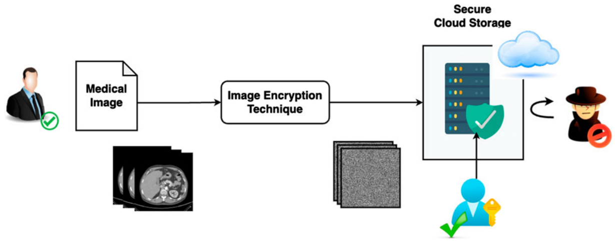


Figure 1. Secure cloud storage flow.

tion methods bring randomness to the image pixels by introducing chaotic maps. These maps are available in different dimensions, and the generated sequences are super sensitive to control parameters and initial values, great ergodicity, and greater pseudo-randomness [6]. As these chaotic sequences demonstrate randomness, scrambling can be introduced among the bit-planes to improve diffusion. Furthermore, to enable space-efficient pixel substitution, DNA encoding presents a viable solution, allowing operations to be conducted over DNA-encoded data [7]. Consequently, a set of image encryption algorithms is proposed by integrating DNA computing with chaotic maps. Those techniques are effective and robust.

However, From the quantum computing standpoint, these schemes are more susceptible to various attacks. More articles are available on quantum image encryption techniques based on traditional, hybrid, and hyperchaotic maps [8]. Leveraging quantum-based chaotic maps can mitigate these vulnerabilities, as quantum gates introduce randomness and variability and enhance security against attacks. In many cases, classical image representations are transformed into quantum image representations prior to encryption, utilizing a variety of representation methods. Numerous studies base their encryption techniques on the specific representation style they employ, yet no standardized representation has been established [9]. Scrambling techniques are adopted in quantum-based image encryption techniques [10]. Added to that, the watermarking technique is also incorporated to improve security [11]. Furthermore, the unique properties of qubits, such as entanglement, provide enhanced robustness against both classical and quantum-based threats. However, most quantum image encryption methods are resource-intensive, complex, and challenging to integrate with classical systems that require quantum-level security. This creates a strong demand for hybrid encryption systems that operate on classical image pixels while maintaining quantum-secure characteristics. Such solutions are particularly sought after in fields like healthcare, where full-scale quantum infrastructure might be impractical, yet the need for quantum-level security remains essential [12].

Hence, this paper introduces a new encryption technique for medical images, QMedShield, integrating quantum-inspired chaotic maps, bit plane scrambling, quantum operations, and hybrid chaotic maps with DNA encoding techniques. Thus, QMedShield can seamlessly integrate with classical healthcare systems, providing quantum-level security with minimal quantum computing resources. The overall block diagram is depicted in Figure 2. The major contributions to the article are outlined below.

(1) A novel medical image encryption scheme, QMedShield, is proposed for their secure storage in the cloud with quantum chaos, quantum operations, hybrid chaos, bit plane scrambling, and DNA encoding.
(2) Pixel diffusion is achieved with bit plane scrambling, classic and quantum chaotic sequences, and quantum operations such as Hadamard and CNOT.
(3) Pixel confusion has been done with hybrid chaotic map sequence and DNA encoding-based pixel substitution.
(4) QMedShield has been validated using three different medical image datasets and demonstrated that the model is secure and attack-resistant with multiple statistical experimental and theoretical analyses.

The subsequent segments of the article are organized as follows: Section 2 discusses the different image encryption schemes available. Preliminary concepts are briefed in Section 3. Section 4 elaborates on the novel encryption algorithm, QMedShield. In Section 5, the security

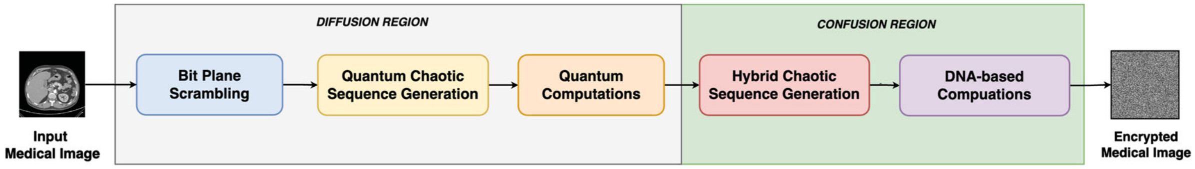


Figure 2. Overall block diagram.

analysis of the introduced encryption model is discussed. In the end, Section 6 presents the paper's conclusion and outlines future directions.

2. Related work

This section explores the existing image encryption schemes and their evolution in recent times. Some survey articles already discuss medical image encryption from different aspects [13]. Through classical image encryption, sensitive visual data is protected from unauthorized access and malicious exploitation. With robust primitives like substitution-permutation networks and Feistel ciphers, classical encryption methods aim to obfuscate image content and resist cryptanalysis. Classical image encryption entails two primary domains: spatial and transform [5]. There are increasingly interesting algorithms utilizing DNA encoding, cellular automata, metaheuristics, chaotic maps, fuzzy logic, and more in the spatial domain. Healthcare is one of the most important domains, and this requires secure and confidential image storage techniques. Priyanka et al. [14] offer a detailed exploration of encryption techniques applicable to healthcare images, along with suggestions for future research directions.

In cryptography, chaotic maps offer a promising avenue for generating secure cryptographic keys by exploiting the chaotic behaviour exhibited by nonlinear dynamical systems [15]. Additionally, chaotic maps serve as effective components in image encryption schemes, where they facilitate the transformation of plaintext images into ciphered forms by introducing complexity and randomness. Different chaotic maps such as 2D Arnald maps [16], Chen [6], and 2D sine-coupling map [17] are used for multiple purposes like confusion, diffusion, random key generation, scrambling, and substitution. Paul et al. [18] developed a unique encryption scheme that integrates hyperchaotic maps and Zaslavskii map-based pixel shifting with SHA-2 algorithm. Recently Yi et al. [19] also introduced a novel image encryption mechanism that leverages classic AES and the latest Rossler hyperchaotic systems. To improve the performance, image compression-based encryption mechanisms are developed [20]. DNA encoding enhances the diffusion rate in image encryption schemes. Similarly, Arthi et al. [21] devised a 4D-hyperchaotic map combined with a DNA-encoding technique and validated with medical images. Moreover, In multimedia, DNA-computing-based encryption techniques have been broadening to cloud applications. Recently, Amaithi Rajan et al. [22] designed an encryption model, particularly for the secure storage and processing of medical images in a cloud server, utilizing hyperchaotic maps, DNA encoding, and bitplane scrambling. The model demonstrates robustness and resistance against attacks, ensuring the security and privacy of sensitive image information.

However, all these techniques are classical cryptography-based, which are easily compromised by quantum computing. So, we are in need of a based image encryption model. Researchers are working in this area also. A framework for the chaos-based quantum encryption of healthcare images that guarantees patient safety and anonymity was presented in an article by Abd El-Latif et al. [23]. Janani et al. [24] proposed a new technique based on quantum image representation and chaotic maps to secure medical images. Different quantum image representations are available, such as GRMMI [10], GQIR [25], FRQI [26]. In quantum image encryption, scrambling techniques and chaotic maps are used to introduce diffusion. Ran et al. [27] injected three impulses during the 3D-hyperchaotic lorenz sequence generation to improve the randomness in the sequence, then used those sequences for quantum image encryption with NCQI representation. Recently, Dai et al. [26] utilized the backpropagation mechanism to generate the Q-logistic sequences for image encryption with a quantum particle swarm optimization strategy.

Based on the insights from the literature review, integrating quantum chaotic maps, quantum computations, bit-plane scrambling, and DNA encoding could increase image encryption security. In line with these findings, we devised a novel image encryption model. Table 1 shows how our method varies from existing methods.

3. Preliminaries

This section outlines the basic definitions of concepts used in the encryption model employed. It covers topics such as bit plane scrambling, different chaotic maps, basic quantum operators, and DNA encoding.

3.1. *Bit plane scrambling*

The bit plane of a digital image comprises an array of bits corresponding to particular bit positions in each of the binary representations of a pixel [22]. For example, in an image where each pixel is represented by 8 bits, there are 8-bit planes. As illustrated in Figure 3, bit plane scrambling rearranges these planes according to a key. The benefits of bit plane scrambling include improving image security by diffusing visual patterns, strengthening defenses against unauthorized access or manipulation, and facilitating encryption efficiency while preserving image fidelity.

Table 1. Our method vs existing methods.

	Chotic Map						
Reference	Classic Chaotic Map	Quantum Chaotic Map	DNA Computing	Quantum Operations	Bit Plane Scrambling	Statistical Attack Resistance	CP/KP Attack Resistance
Arthi et al. [21]	√		√			√	√
Amaithi Rajan et al. [22]	√		√		√	√	√
Dai and Zhou [26]		√		√		√	
Zhou et al. [28]	√			√		√	
Houshmand et al. [29]	√			√		√	
Ours	√	√	√	√	√	√	√

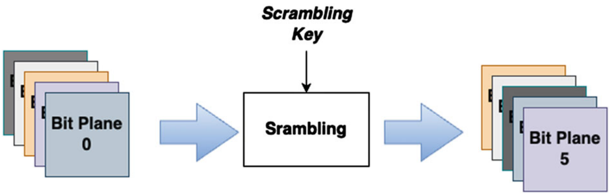


Figure 3. Bit plane scrambling.

3.2. Chaotic maps

Chaotic maps explore the behaviours of dynamic systems that often express non-linear randomness. They are categorized into two types: 1D and nD systems. They are too sensitive to initial conditions. This implies that outputs can be drastically altered by slightly changing the initial parameters. Chaotic maps can be categorized into discrete and continuous maps, both serving to generate keys for pixel diffusion in images. We employ a 2D Henon map, a hybrid logistic-sine map, and a 3D quantum logistic map in the proposed encryption algorithm. Subsequent subsections provide a comprehensive explanation of the logic behind these chaotic maps.

3.2.1. Henon chaotic map

Henon map is a 2D quadratic chaotic map [30]. This Henon 2D chaotic map provides significant advantages over 1D chaotic maps in image encryption models. Its two-dimensional nature enables richer and more complex chaotic behaviour, leading to increased security and robustness against cryptanalysis. Moreover, the Henon map's strong nonlinear behaviour introduces randomness and complexity into the encryption process, improving the security of the encrypted image. Its efficient diffusion properties ensure that changes to individual pixels propagate effectively, enhancing the overall security and cryptographic strength of the encryption model. This map is defined using the Equations (1) and (2) below.

$$x_{n+1} = 1 - \alpha x_n^2 + y_n \tag{1}$$

$$y_{n+1} = \beta x_n \tag{2}$$

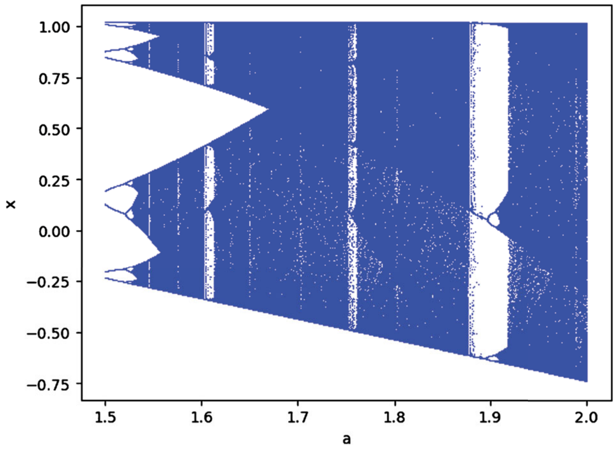


Figure 4. Bifurcation diagram of Henon Map: $\beta = 0.3$.

The traditional Henon map expresses chaotic behaviour with parameter values of $\alpha = 1.8$ and $\beta = 0.3$. However, varying these parameters will result in different chaotic behaviours. Figure 4 shows the bifurcation diagram of the Henon map.

3.2.2. Hybrid chaotic map

Hybrid chaotic maps are mathematical constructs that merge various chaotic systems or maps to produce complex and adaptable dynamical patterns [31]. By leveraging techniques such as sequential or parallel coupling, these hybrid maps show heightened intricacy and volatility beyond what their individual components provide. The integration of these maps aims to foster more convoluted dynamics, amplify randomness, or enhance specific attributes of chaotic behaviour. The logistic-sine map is utilized in our model to generate the sequence used in the confusion region. The system equation of the logistic-sin map is as follows.

$$x_{n+1} = rx_n(1 - x_n) + 4r.\sin\left(\frac{\pi x_n}{4}\right) \tag{3}$$

When r varies from 0.6 to 1.2, the map shows chaotic behaviour. Figure 5 illustrates the Hybrid map's bifurcation diagram.

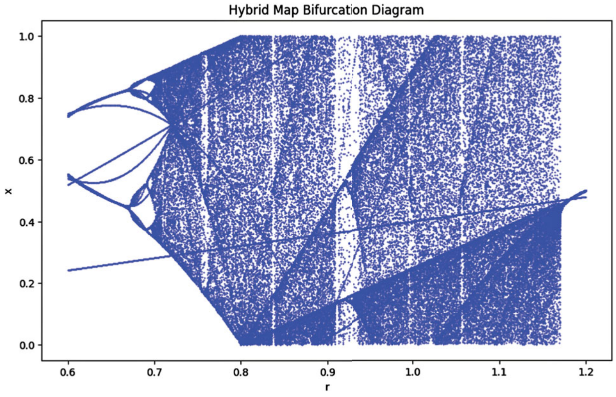


Figure 5. Hybrid logistic-sin map bifurcation diagram.

3.2.3. 3D quantum logistic chaotic map

Similar to traditional 3D chaotic maps [15], quantum-inspired chaotic maps demonstrate heightened levels of complexity and unpredictability. Although the 3D Quantum Logistic Chaotic Map incorporates concepts inspired by quantum mechanics, it operates in a classical setting without relying on quantum states. Instead, it leverages quantum-like chaotic dynamics through complex numbers and non-linear interactions. This makes it suitable for applications in chaos-based cryptography, where its chaotic dynamics can generate secure cryptographic keys. Equations (4)–(6) represent the 3D Quantum Logistic Chaotic Map, which offers distinct characteristics compared to classical chaotic maps like the 3D Lorenz map.

$$x_{n+1} = \eta(x_n - |x_n|^2) - \eta y_n \tag{4}$$

$$\begin{aligned} y_{n+1} = {} & -y_n e^{-2\gamma} + e^{-\gamma}\,\eta[(2 - x_n - x_n^*)y_n \\ & - x_n z_n^* - x_n^* z_n] \end{aligned} \tag{5}$$

$$z_{n+1} = -z_n e^{-2\gamma} + e^{-\gamma}\,\eta[2(1 - x_n^*)z_n - 2x_n y_n - x_n] \tag{6}$$

In this equation, γ denotes the dissipation parameter, η stands for the control parameter, and x_n^*, y_n^* represent the complex conjugates of x_n, y_n. The state of equations is chaotic when $\eta = 4$,$x_n \in (0, 1], y_n \in (0, 0.1], z_n \in (0, 0.2], \gamma \in [6, +\infty]$. Figure 6 shows the phase diagrams of the used quantum logistic map to demonstrate its randomness.

This distinction influences their suitability for different applications, with the quantum logistic map designed for enhanced security in classical cryptographic systems.

3.3. Quantum operations

In the evolving quantum age, leveraging qubits rather than using classical bits in image encryption provides enhanced security through the principles of quantum mechanics. Quantum operators such as the Hadamard and CNOT gates offer unique benefits: the Hadamard gate allows for the formation of superposition states, enabling efficient encoding and manipulation of information, while the CNOT gate facilitates controlled operations between qubits, essential for implementing complex encryption algorithms [29]. These quantum gates improve the performance of encryption schemes, offering increased randomness and variability in the encryption process, thus strengthening the security posture against cryptographic attacks. Additionally, the inherent properties of qubits, including entanglement and the ability to represent and process information in a fundamentally different way than classical bits, contribute to the robustness of image encryption schemes in the quantum domain. Through the integration of quantum operators, image encryption systems can achieve higher levels of security and resilience against both classical and potential quantum threats.

3.3.1. Hadamard gate

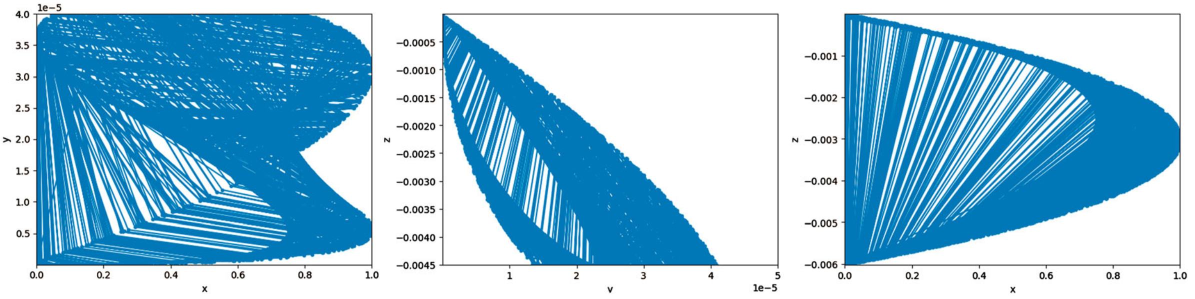
The Hadamard gate serves as a fundamental quantum gate for generating superposition states. Upon application to a qubit, it transforms a basis state $|0\rangle$ into an equal superposition of $|0\rangle$ and $|1\rangle$, and vice versa. Mathematically, it represents a rotation of the qubit's state vector by 90 degrees around the x-axis of the Bloch sphere. The Hadamard gate plays a crucial role in quantum algorithms, such as quantum Fourier transforms and quantum search algorithms, by generating and manipulating superposition states. Its application enables quantum computers to efficiently process information in parallel and perform certain calculations more effectively than classical computers. Quantum circuit of the $\mathcal{H}$ gate is shown in Figure 7(a), and the Hadamard matrix is described by

$$\mathcal{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{7}$$

Figure 7(b) illustrates that when a qubit is set to the state $|0\rangle$ at first, subject to the $\mathcal{H}$ gate operation, it moves a superposition state where the probabilities of estimating 0 and 1 are equal. The optical implementation of the $\mathcal{H}$ gate is shown in Figure 7(c).

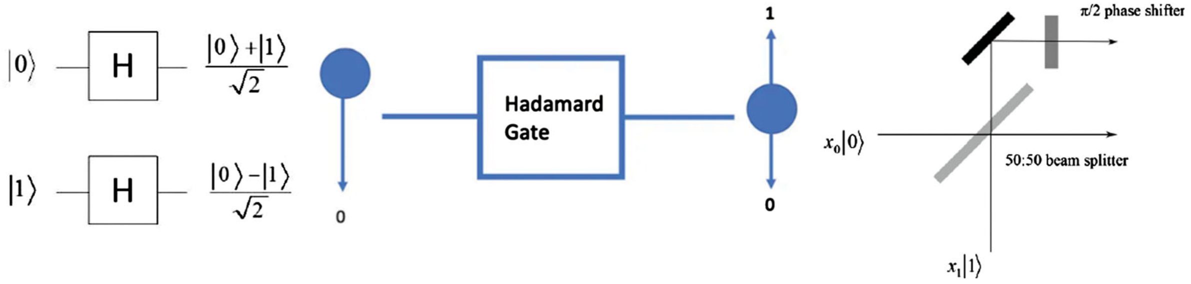
3.3.2. CNOT gate

The Controlled-NOT (CNOT) gate is a basic gate used for entangling qubits and implementing controlled operations in quantum computing. The CNOT gate functions on two qubits, with one serving as the control and the other as the target. When the control qubit is in state $|1\rangle$, the CNOT gate flips the state of the target qubit.



(a) (b) (c)

Figure 6. Phase diagrams of quantum logistic map. (a) *xy* plane. (b) *yz* plane and (c) *xz* plane.



(a) (b) (c)

Figure 7. Hadamard gate representations.

However, if the control qubit is in state |0⟩, the target qubit remains unaffected. The CNOT gate is essential for creating entanglement between qubits, enabling the execution of quantum algorithms such as quantum teleportation and error correction. Its versatility makes it a cornerstone in quantum computation and communication protocols. It is the same as the XOR operation in classical computation. However, The CNOT operation enhances security by entangling qubits, creating interdependent states that are challenging to separate or replicate. This operation leverages superposition, adding complexity and unpredictability that make it difficult for attackers to infer original data. Additionally, any attempt to measure qubits collapses their states, providing inherent protection against eavesdropping, a level of security not achievable with classical XOR. The CNOT matrix representation is shown in Equation (8). Figure 8 visualizes the quantum circuit of the CNOT gate.

$$\mathcal{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{8}$$

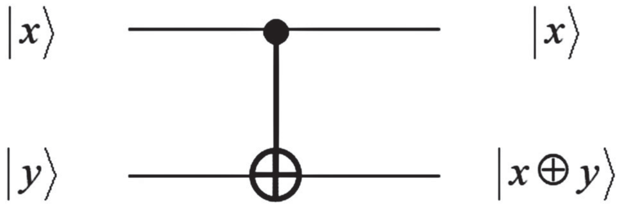


Figure 8. CNOT quantum circuit.

3.4. DNA encoding

DNA encoding involves representing digital data using the four nucleotide bases of DNA which are adenine(A), guanine(G), cytosine(C), and thymine(T), instead of binary digits. This technique utilizes the unique properties of DNA molecules, such as their high storage capacity and stability, for data storage and computation. A DNA sequence could be generated from binary data. DNA computing holds significant promise in image cryptography due to its ability to leverage massive parallelism, high data density, robustness, and unique security properties. By encoding image data into DNA sequences, DNA-based encryption schemes can efficiently process large-scale image data while ensuring secure storage and transmission. Arithmetic and logical operations can also be executed on DNA-encoded information, with the truth table of the DNA XOR operation presented in Table 2.

4. Proposed encryption model

The proposed QMedShield: a Quantum chaos-based image encryption model, is explained in detail in this section. The detailed introduced encryption flow is

Algorithm 1 QMedShield: Quantum Chaos-based Medical Image Encryption

```
Input: Medical Image $Med_i$, Secret Key $K = \{k_1, k_2, \ldots, k_{18}\}$ Output: Encrypted Medical Image $CMed_i$
Convert $Med_i$ to 8-bit planes: $Med_i = \{b_{i0}, b_{i1}, \ldots, b_{i7}\}$
Diffusion Region
Step 1: Generate Keys
Derive $bp_k, ks_k$ from Henon map using $(x_0 = k_1, y_0 = k_2, r)$ per Equation (1)- -(2)
Step 2: 3D Quantum Logistic Map
Set $(x_0 = k_3, y_0 = k_4, z_0 = k_5)$; compute $x_i, y_i, z_i$ per Equation (4)- -(6)
Obtain $K_X, K_Y, K_Z$ using $x_i, y_i, z_i$ per Equation (9)- -(11)
Step 3: Scrambling
Scramble $Med_i$ with $bp_k$: $SI_i = \{SI_{i0}, SI_{i1}, \ldots, SI_{i7}\}$
Select $K_S$ from $\{K_X, K_Y, K_Z\}$ based on $ks_k$
Step 4: Quantum Entanglement and Diffusion
Apply $\mathcal{H}$ and CNOT gates on $SI_i$ and $K_S$ in a quantum circuit
Measure the values, resulting in $C_i$
Step 5: DNA Encoding
Encode $C_i$ to DNA planes $DN_i = \{DN_{i0}, DN_{i1}, DN_{i2}, DN_{i3}\}$ using $k_6$- -$k_9$
Confusion Region
Step 6: Hybrid Logistic-Sine Map
Generate $K_H$ with $x_0 = k_{10}$ per Equation (3); match size to $Med_i$
Step 7: DNA Encoding of $K_H$
Encode $K_H$ as DNA planes $DK_i = \{DK_{i0}, DK_{i1}, DK_{i2}, DK_{i3}\}$ using $k_{11}$- -$k_{14}$
Step 8: DNA XOR
$DX_i \leftarrow DNA\_XOR(DN_{ik}, DK_{ik}),\ k = 0, 1, 2, 3$
Step 9: DNA Decoding
Decode $DX_i$ using $k_{15}$- -$k_{18}$ to get $CMed_i$
return $CMed_i$
```

Table 2. DNA XOR truth table.

XOR	A	G	T	C
T	T	C	A	G
G	G	A	C	T
A	A	G	T	C
C	C	T	G	A

shown in Figure 9. Key Management Centre (KMC) generates the keys to share with users.

The proposed model is founded on the permutation-diffusion model of Shannon, which forms the fundamental basis. QMedShield has two regions to be processed. One is the diffusion region where image bit planes are scrambled and pixel values are diffused using a generated key with quantum operations. Another one is the confusion region, where pixel substitution using DNA encoding and XOR operations takes place. Both regions are explained in the following Subsections 4.1 and 4.2. The following Algorithm 1 shows the steps to be processed in QMedShield in brief. The Medical Image Med_i and secret key $K = \{k_1, k_2, k_3, k_4, \ldots, k_{18}\}$ from KMC are given to the authorized image owners who can encrypt the medical image data. The resultant Cipher Medical Image $CMed_i$ will be offloaded to the cloud for secure storage.

4.1. QMedShield: diffusion region

The pixel diffusion region in image encryption enhances security by spreading pixel values across the image, minimizing patterns, and making the ciphertext less predictable. This process ensures that minor changes in the plaintext image result in significant alterations in the encrypted output, strengthening resistance to attacks.

In our diffusion region, the grayscale input medical image is read as in 8-bit plane format, $Med_i = \{b_{i0}, b_{i1}, b_{i2}, \ldots, b_{i7}\}$. Then, the bit plane scrambling key (bp_k) and key selection key (ks_k) are derived by giving initial parameters $x_0 = k_1, y_0 = k_2$ and seed r to the Henon map as described in Equations (1)–(2). It is assumed that the value of r is confidentially shared by the receiver and sender of the medical image. For the secure key generation, 3D quantum logistic map sequences are generated from the chaotic system represented by Equations (4)–(6) by feeding the initial parameters $x_0 = k_3, y_0 = k_4, z_0 = k_5$. Each sequence matches the size of an image Med_i.

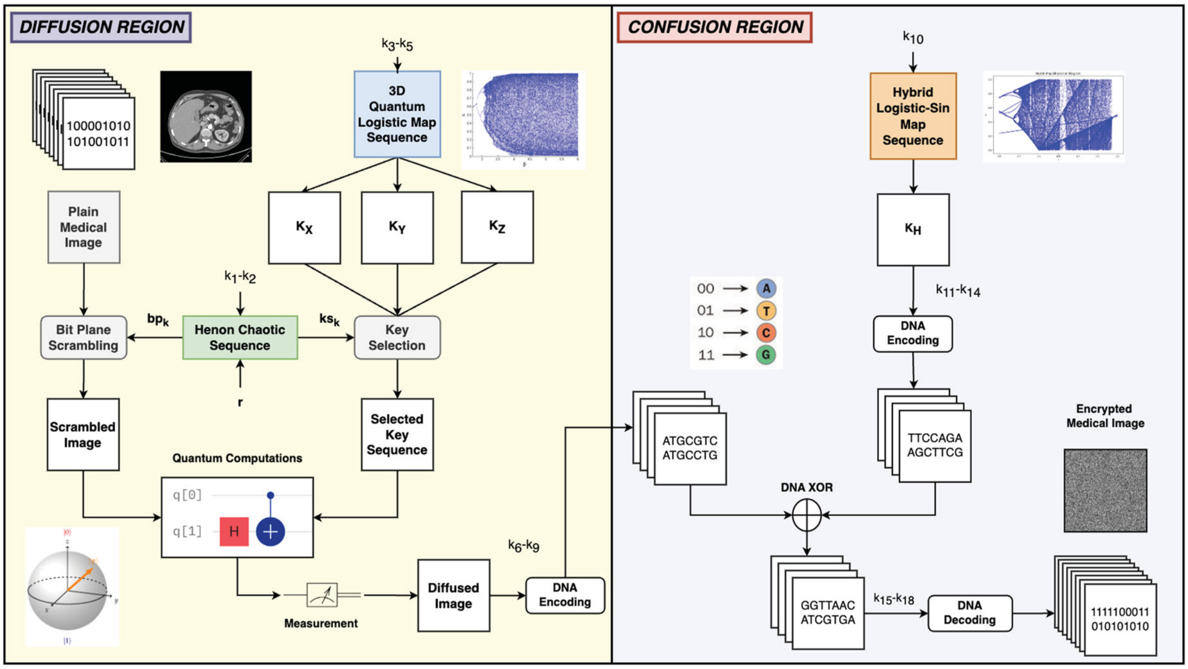


Figure 9. Flow diagram of the image encryption.

These matrices are the diffusion keys, and they are computed leveraging the given Equations (9)–(11). where (ϵ_1, ϵ_2) denote two large prime numbers and x_i, y_i, z_i represents random sequences, generated using 3D quantum logistic map.

$$K_X = mod(floor(\epsilon_1 x_i + \epsilon_2), 256) \tag{9}$$

$$K_Y = mod(floor(\epsilon_1 y_i + \epsilon_2), 256) \tag{10}$$

$$K_Z = mod(floor(\epsilon_1 z_i + \epsilon_2), 256) \tag{11}$$

During the diffusion, Med_i is being scrambled using bp_k, outputs scrambled image $SI_i = \{SI_{i0}, SI_{i1}, SI_{i2}, SI_{i3}, \ldots.., SI_{i7}\}$. Meanwhile, from the three quantum logistic keys, one key K_S is randomly selected based on ks_k. Instead of representing the whole image in quantum image representation, which is more quantum computing resource-intensive, during the diffusion region, corresponding pixels from SI_i and K_S are converted into qubits and fed into a quantum circuit. This design is less resource-intensive. In a quantum circuit, the chosen key K_S and the scrambled image SI_i undergo $\mathcal{H}$ transformation with CNOT gate to create an entangled qubit. This process comprises applying a $\mathcal{H}$ gate and then a CNOT gate to convoy all values in the resulting matrices to a superposition state and establish entanglement. It is called so quantum XOR. The quantum state of the diffused grayscale pixel of the image is collapsed into their classical versions by the quantum measurement process, denoted as C_i. The obtained diffused image C_i is transformed into DNA encoded 4 planes $DN_i = \{DN_{i0}, DN_{i1}, DN_{i2}, DN_{i3}\}$ using $k_6 - k_9$.

In this region, quantum XOR operation increases ciphertext entropy and unpredictability. The quantum XOR operation involves a Hadamard gate ($\mathcal{H}$), which transforms a qubit into a superposition, defined as $\mathcal{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and a CNOT gate, which entangles a control qubit $|SI\rangle$ with a target qubit $|K'\rangle$. The encryption algorithm is expressed as $CMed = Enc(Med, K) + \text{QXOR}$. This *QXOR* increases the unpredictability for an attacker has been proved with the following Theorem 4.1.

Theorem 4.1: *The quantum-based XOR operation using Hadamard and CNOT gates enhances the security of an encryption algorithm by increasing ciphertext complexity and providing resilience against known plaintext attacks.*

Proof: Let *Med* represent the plaintext image, *SI* is the scrambled image of *Med* and *K* the key. The initial ciphertext image without QXOR is defined as $CMed_0 = Enc(Med, K)$. Converting K into a qubit $|K\rangle$ and applying the Hadamard gate gives $|K'\rangle = \mathcal{H}|K\rangle$. The CNOT gate is then applied, resulting in an entangled state $\text{CNOT}(|SI\rangle, |K'\rangle)$. After performing the quantum XOR operation, the resulting state is

$$|CMed\rangle = |SI\rangle \oplus |K'\rangle. \tag{12}$$

The application of quantum operations increases the entropy of the ciphertext, expressed as

$$Ey(CMed) = Ey(SI) + Ey(K'), \tag{13}$$

thereby enhancing randomness. It is evident that $Ey(CMed) > Ey(CMed_0)$. In a known plaintext attack scenario, an adversary possessing both *Med* and *CMed* cannot easily derive the relationship due to the complexity introduced by quantum XOR.

The effective key space is expanded as 2^n for n qubits, making brute-force attacks less feasible. Small modifications in *Med* or *K* yield significantly different ciphertext outputs, amplifying the avalanche effect. Integrating quantum XOR operations using Hadamard and CNOT gates into the encryption algorithm significantly enhances the unpredictability and complexity of ciphertext generation. This integration strengthens resistance to known plaintext attacks and expands the effective key space. ■

4.2. QMedShield: confusion region

The pixel confusion region in image encryption rearranges pixel positions to obscure the original image structure, preventing attackers from identifying patterns. This scrambling process enhances security by making it difficult to trace pixel values back to their original locations. In QMedShield, a hybrid logistic-sine map sequence K_H is generated using Equation (3) by giving the initial parameter $x_0 = k_{10}$. The sequence length is the same as the size of Med_i. The generated key K_H is converted into DNA encoded 4 planes $DK_i = \{DK_{i0}, DK_{i1}, DK_{i2}, DK_{i3}\}$ using $k_{11} - k_{14}$. This DNA encoding process achieves pixel confusion. Finally, the DNA XOR image DX_i is DNA decoded using $k_{15} - k_{18}$ and produces the encrypted medical image $CMed_i$.

In the QMedShield, harnessing qubits instead of classical bits in image encryption enhances security through quantum operators like the Hadamard and CNOT gates. This has been proved in Theorem 4.1. The Hadamard gate enables superposition states, facilitating efficient encoding, while the CNOT gate allows controlled operations between qubits, which is crucial for complex encryption algorithms. These quantum gates reinforce encryption schemes by introducing randomness and variability, thereby fortifying security against attacks. The decryption process involves reversing the given steps. The original medical image *Med* can be reconstructed using the equation below, and the process flow is illustrated in Figure 10.

$$Med_i = Decryption(CMed_i, K, r) \tag{14}$$

5. Experimental results and analysis

This section is dedicated to analyzing the proposed encryption model. We have outlined the experimental setup, including the medical dataset used for analysis, and presented various experimental results accordingly. This includes analyses such as statistical attack analysis, key security analysis, analyses of resistance to chosen plaintext and known plaintext attacks, and differential attack analysis.

5.1. Experimental setup and dataset

The designed encryption model was implemented on a PC with an Intel Xeon processor, 64 GB RAM, 16 GB of memory with an NVIDIA Quadro P5000 GPU, and a 64-bit Windows operating system. Python OpenCV libraries and Qiskit have been used in the development of the entire system. Three different medical image datasets were chosen to experiment with and evaluate the proposed algorithm. Details of the dataset have been explained briefly here,

- **Brain Tumor MRI Dataset (BMRI) [32]:** The three datasets below are combined to create this dataset: figshare, SARTAJ, Br35H. There are 7023 MRI images of the human brain in this collection, divided into 4 categories: pituitary, glioma, meningioma, and no tumour. Images categorized as the 'no tumor' class were obtained from the Br35H dataset.
- **Chest X-ray Dataset (CXR) [33]:** This dataset originates from the NIH, which is the largest chest radiograph data set. From 30,805 special patients, 112,120 frontal X-ray images are collected. Each X-ray is linked to the associated text disease label, which is drawn from the relevant radiological reports using an NLP algorithm.
- **Lung Cancer CT Dataset (LCT) [34]:** From different specialist hospitals, the IQ-OTH/NCCD lung cancer dataset was collected over three months in the fall of 2019. It comprises CT scans from patients with lung cancer in different stages and healthy subjects, totalling 1190 images from 110 cases. The dataset, marked by oncologists and radiologists, categorizes cases into three classes: normal (55 cases), benign (15 cases), and malignant (40 cases).

The proposed QMedShield's security is evaluated using a number of metrics, and it has been proven that it is resistant to various cryptographic attacks, including brute-force attacks, statistical attacks, histogram attacks, and differential attacks. Throughout the section, 6 sample medical images $BMRI_1, BMRI_2, CXR_1, CXR_2, LCT_1, LCT_2$ are taken (2 images from each dataset) to show the performance comparison. The selection of MRI, X-ray, and CT images for the encryption task aims to demonstrate the versatility and effectiveness of our model across

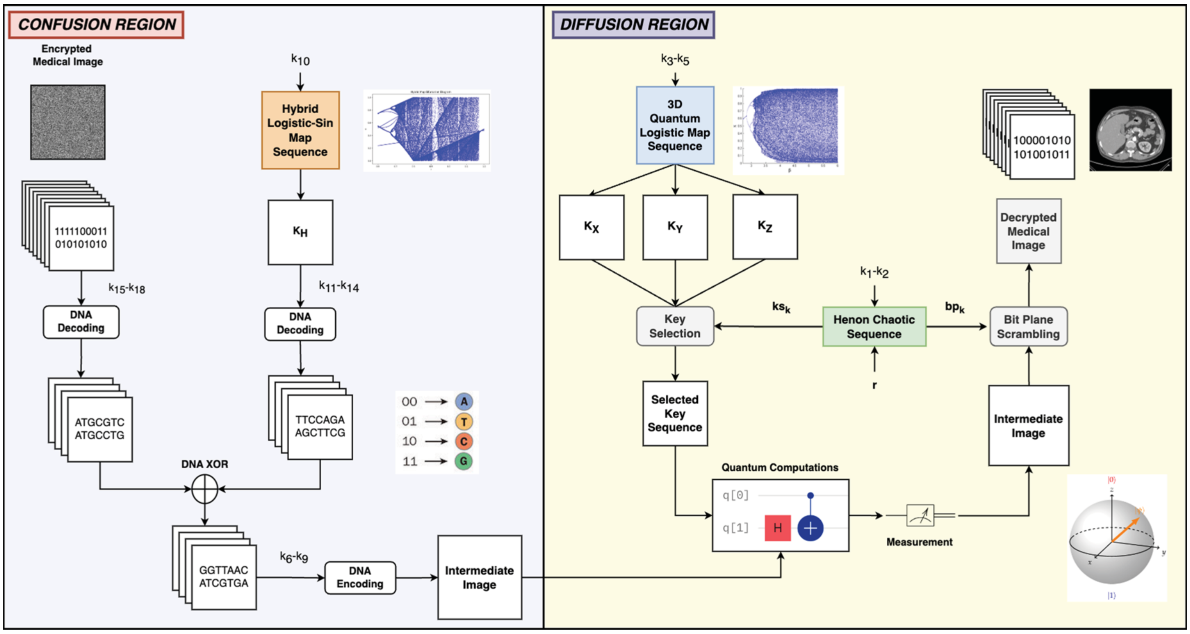


Figure 10. Flow diagram of the image decryption.

various imaging modalities, showcasing its applicability and robustness in diverse clinical scenarios. Figure 11 shows the selected sample medical images and their corresponding encrypted images.

5.2. Key space analysis

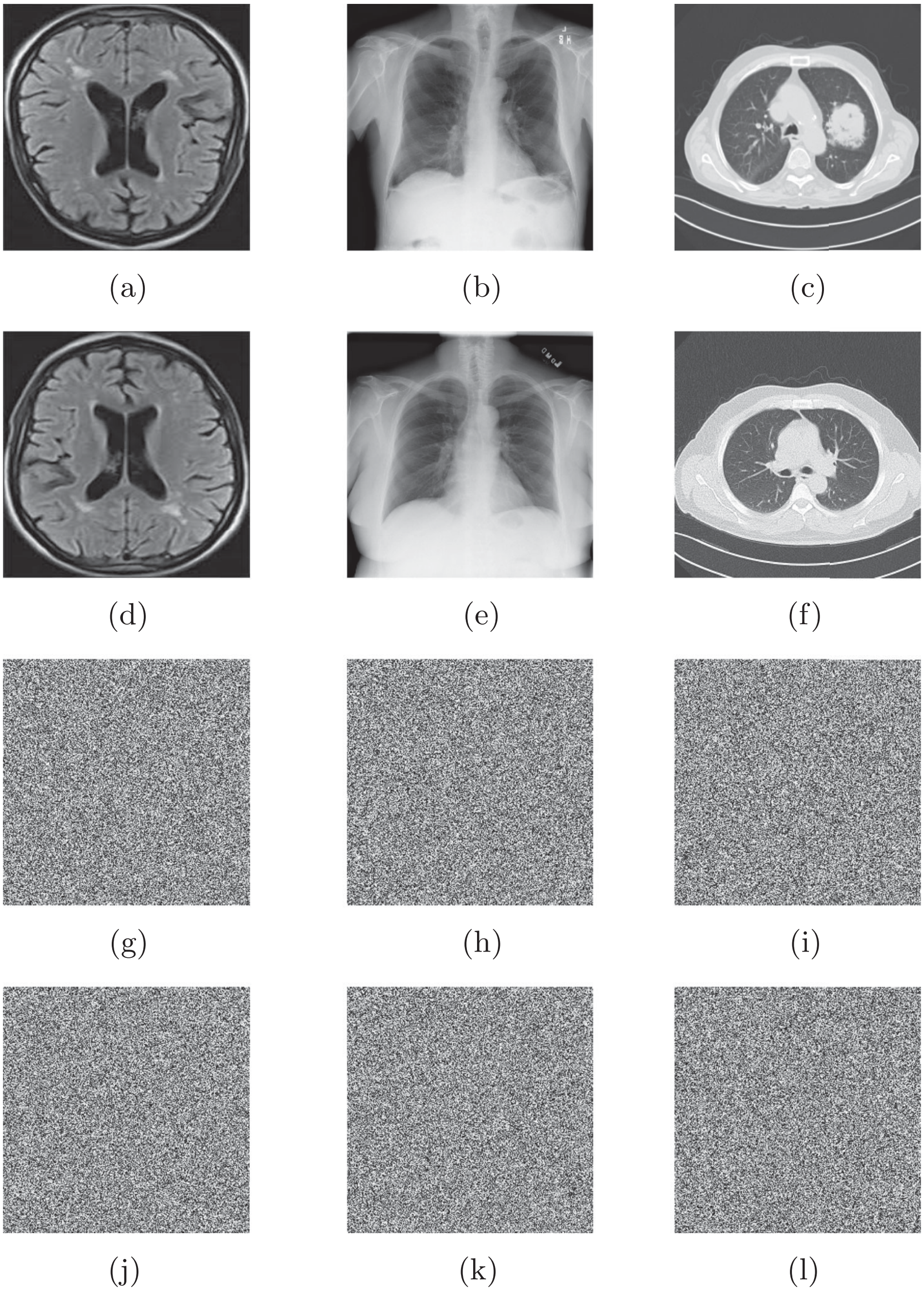
In contemporary cryptography, the magnitude of the key space plays an important role in discovering the resilience of a crypto model against brute-force attacks [35]. To thwart such attacks, robust passphrases or passwords and encryption models boasting adequately expansive key capacities are indispensable. It is commonly recommended to maintain a space of at least 2^{128} to withstand brute-force endeavours [22]. Typically, a larger key space renders it increasingly arduous to deduce the exact security key through brute force, thereby augmenting the security of the model. The key volume computation hinges on the count of unique keys employed in both the confusion and diffusion stages. In a chaotic map, initial values and control parameters serve as keys. For the proposed QMedshield scheme, the private key encompasses a collection of initial conditions and control parameters, delineated as follows: 1) Henon chaotic map has $(x_0, y_0, \alpha, \beta)$. 2) Hybrid logistic-sin map has (x_0, r). 3) 3D quantum logistic map have $(x_0, y_0, z_0, \eta, \gamma)$. The proposed encryption scheme has 11 keys used to generate chaotic sequences that are more sensitive and have large key space. Let's say the precision is 10^{-14} (i.e. double precision (2^{52})), then the size of key space will be equal to $2^{52} * 11 = 2^{572} > 2^{128}$. The findings indicate that the method is significantly resilient to brute-force attacks and demonstrate the difficulty of successfully breaching it through this method.

5.3. Key sensitivity analysis

The encryption algorithm ought to be sensitive to the key. Even minor alterations to the key should result in an entirely different cipher image. The proposed QMedShield demonstrates a high level of sensitivity to the key. The original medical image LCT_2 is shown in Figure 12(a). LCT_2 is encrypted with initialization values for quantum logistic chaotic map $x_0 = 0.5$, $y_0 = 0.05$, and $z_0 = 0.02$. Encrypted LCT_2 is shown in Figure 12(b). If we use the same values while decrypting, we will get the exact original medical image LCT_2 (Refer Figure 12(c)). Figure 12(d) shows the result of decryption if y_0 is given as 0.005. It explains that even a small modification can have a significant impact. Therefore, it ensures guessing the encryption key completely makes it difficult to decrypt.

5.4. Histogram analysis

The statistical properties of the image are represented through the histogram. It counts the number of pixels and primarily displays the distribution of pixel values within the image. A uniform distribution results in a flat histogram, indicating that pixel values are nearly equal throughout the image. Histogram analysis plays a



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Figure 11. Selected sample plain medical images and the corresponding encrypted cipher images. (a) $BMRI_1$. (b) CXR_1. (c) LCT_1. (d) $BMRI_2$. (e) CXR_2. (f) LCT_2. (g) $E(BMRI_1)$. (h) $E(CXR_1)$. (i) $E(LCT_1)$. (j) $E(BMRI_2)$. (k) $E(CXR_2)$ and (l) $E(LCT_2)$.

critical role in both image processing and encryption, serving as a key statistical measure to validate encryption scheme security against statistical attacks. Its widespread use underscores its robust defense against such attacks. The histograms of sample plain images are shown in Figure 13(a–f). The corresponding image's encrypted image histograms are displayed in Figure 13(g–l). The pixel values in the cipher image are uniformly distributed. This experiment demonstrates how pixel value distribution in the original image can be effectively hidden by the cipher image. It protects the data from histogram-based statistical attacks.

5.5. Chi-square test

The chi-square (χ^2) test is used to assess the histogram's evenness. It is calculated using the following Equation (15).

$$\chi^2 = \Sigma_{k=0}^{255} \frac{(OB_k - EX_k)^2}{EX_k} \tag{15}$$

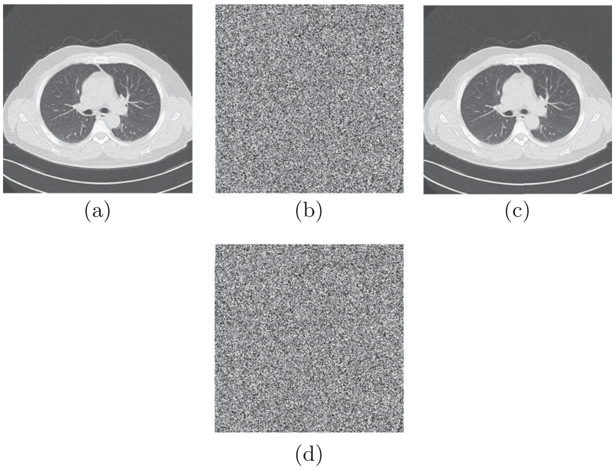


Figure 12. Key sensitivity analysis. (a) LCT_2. (b) Encrypted LCT_2. (c) Decrypted (LCT_2) with $y_0 = 0.05$ and (d) Decrypted (LCT_2) with $y_0 = 0.005$.

Table 3. χ^2 test.

Image	χ^2 Value	Critical Value	Decision ($H = 0$)
$BMRI_1$	261.63	293	Pass
$BMRI_2$	273.04	293	Pass
CXR_1	274.57	293	Pass
CXR_2	264.06	293	Pass
LCT_1	265.49	293	Pass
LCT_2	275.76	293	Pass

In this context, the null hypothesis posits that 'Pixels are evenly distributed'. A critical value denoted as $\chi^2(255, 0.05) = 293$. If the χ^2 value is lower than 293, it is concluded that the null hypothesis is valid and accepted. In Equation (15), OB, EX refers to the observed and expected, respectively. Table 3 shows the χ^2 test done over the sample images.

5.6. Pixel correlation analysis

In image encryption, horizontal, vertical, and diagonal correlation analyses examine the statistical relationships between pixels along different directions within the encrypted image. These analyses provide insights into the spatial distribution of pixel intensities, aiding in the evaluation of encryption effectiveness and the detection of artifacts. By assessing correlation patterns in these directions, encryption practitioners can identify vulnerabilities and optimize algorithms to enhance security and preserve image quality. Equations (16)–(19) can be used to get the correlation coefficient of an image in any direction. In our case, 3 directions: horizontal, vertical, diagonal.

$$Exp(x) = \frac{1}{m} \Sigma_{i=1}^{m} x_i \tag{16}$$

$$D(x) = \frac{1}{m} \Sigma_{i=1}^{m} (x_i - Exp(x))^2 \tag{17}$$

$$Cov(x, y) = \frac{1}{m} \Sigma_{i=1}^{m} (x_i - Exp(x))(y_i - Exp(y)) \tag{18}$$

$$\rho_{xy} = \frac{Cov(x, y)}{D(x)D(y)} \tag{19}$$

The Sub-Figures 14(a–f) clearly show the randomness in Horizontal, Vertical, and Diagonal directions of the plain and encrypted images of selected medical image samples. The correlation coefficients for all 3 directions are presented in Table 4, demonstrating the statistical attack resistance of the proposed encryption scheme on the selected sample medical images.

5.7. Differential attack analysis

The sensitivity of the encryption technique to even minor changes in the plain image is evaluated using the differential attack. The Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) are the two most important performance metrics to assess the proposed technique's resistance to differential attacks. NPCR decides the pixel rate in the encrypted images whenever a single pixel of the test image is changed. It is employed to evaluate the resistance to differential attack. Higher than 99% is the ideal value of NPCR. NPCR is calculated using the following Equations (20) and (21).

$$NPCR = \frac{\Sigma_{p,q} DF(p, q)}{\mathcal{W} \times \mathcal{H}} \times 100\% \tag{20}$$

Here,

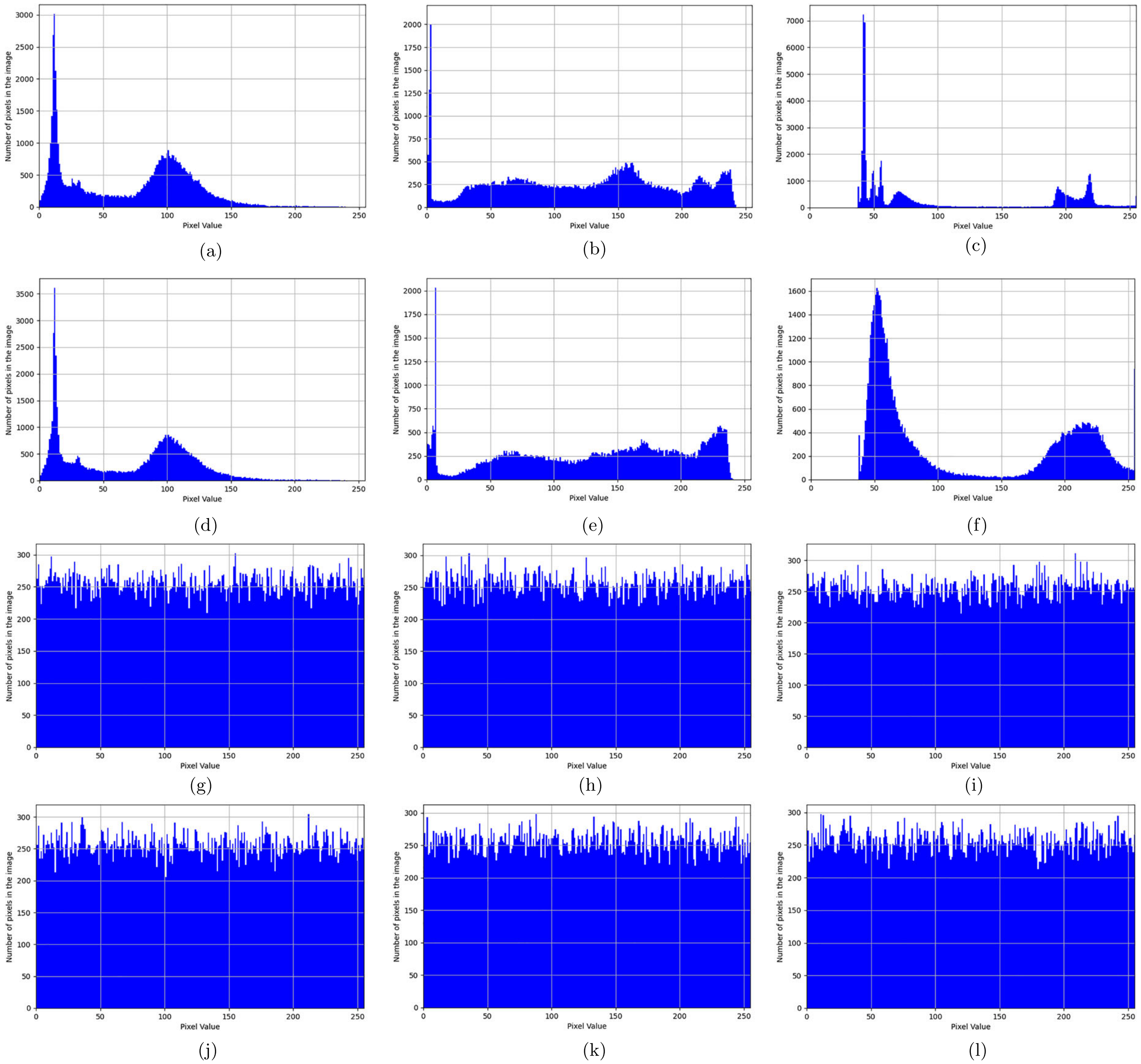
$$DF(p, q) = \begin{cases} 1, & \text{if } Med(p, q) \text{ equals } CMed(p, q) \\ 0, & \text{if } Med(p, q) \text{ not equals } CMed(p, q) \end{cases} \tag{21}$$

where $\mathcal{W}$ and $\mathcal{H}$ denote the width and height of the image. $DF(p, q)$ is the function that calculates the difference between the respective pixels of the original medical image Med and the encrypted medical image $CMed$.

The Unified Average Changing Intensity (UACI), quantifies the average disparity in pixel intensity between the original and encrypted images. This metric is frequently utilized to indicate resilience against a differential attack. An optimal UACI value hovers around 33%, calculated according to Equation (22).

$$UACI = \frac{\Sigma_{p,q} Med(p, q) - CMed(p, q)}{255 \times \mathcal{W} \times \mathcal{H}} \times 100\% \tag{22}$$

Table 5 shows the NPCR and UACI of the sample medical images and proves the withstanding power of the proposed encryption algorithm.



(a)

(b)

(c)

(d)

(e)

(f)

(g)

(h)

(i)

(j)

(k)

(l)

Figure 13. Histogram analysis. (a) Original($BMRI_1$). (b) Original(CXR_1). (c) Original(LCT_1). (d) Original($BMRI_2$). (e) Original(CXR_2). (f) Original(LCT_2). (g) Encrypted($BMRI_1$). (h) Encrypted(CXR_1). (i) Encrypted(LCT_1). (j) Encrypted($BMRI_2$). (k) Encrypted(CXR_2) and (l) Encrypted(LCT_2).

Table 4. Correlation analysis.

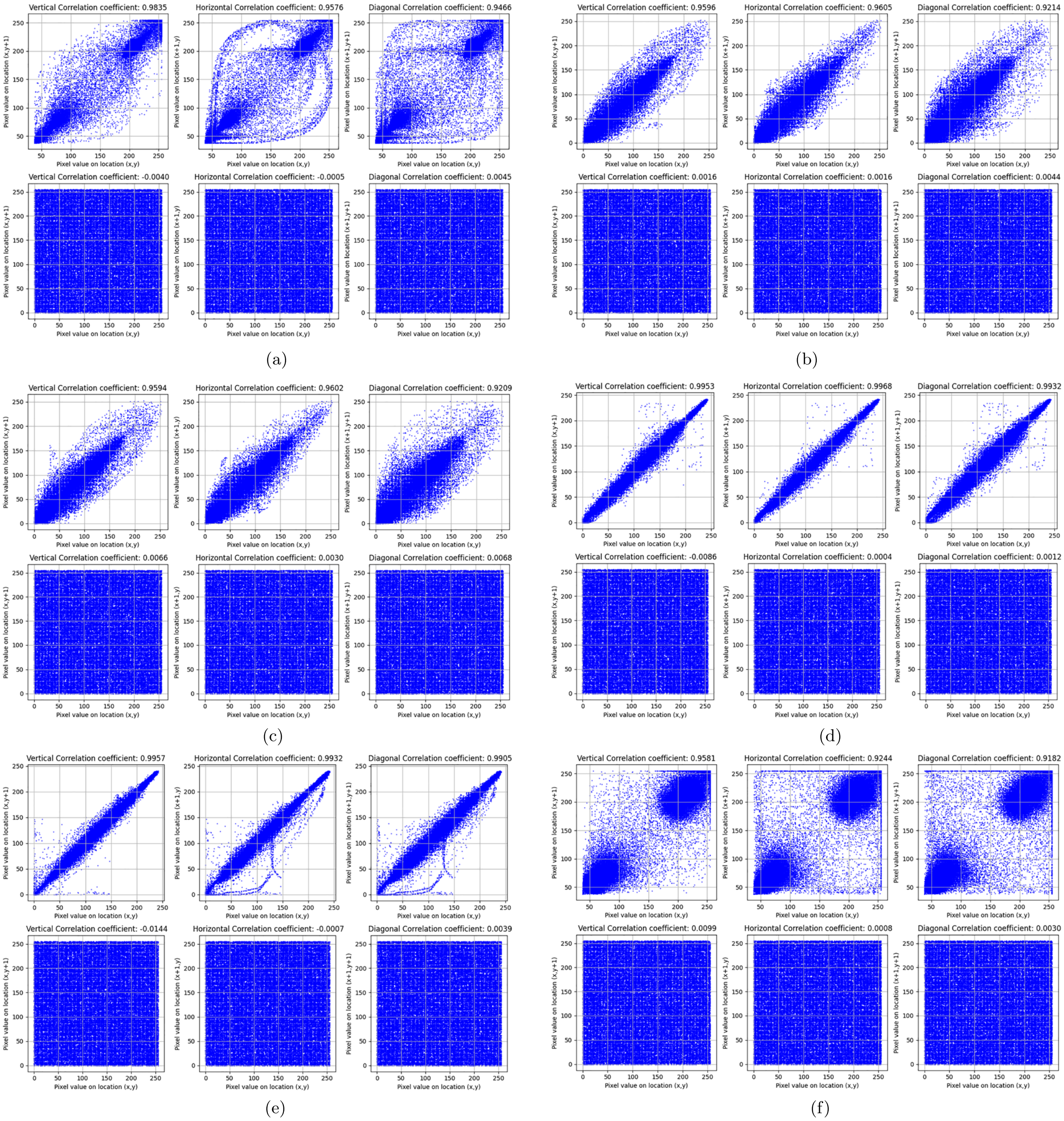
	Horizontal Correlation		Vertical Correlation		Diagonal Correlation	
Image	Original	Encrypted	Original	Encrypted	Original	Encrypted
$BMRI_1$	0.9596	0.0016	0.9605	0.0016	0.9214	0.0044
$BMRI_2$	0.9540	0.0036	0.9593	0.0074	0.9787	−0.1184
CXR_1	0.9929	−0.0002	0.9929	−0.0088	0.9973	−0.0776
CXR_2	0.9957	−0.0144	0.9932	0.0007	0.9905	0.0039
LCT_1	0.9835	−0.0040	0.9576	−0.0005	0.9466	0.0045
LCT_2	0.7084	0.0002	0.9553	0.0107	0.9482	−0.0075

5.8. Entropy analysis

Entropy characterizes the unpredictability of image information, denoted by Ey. It serves to measure the uncertainty inherent in the proposed encryption technique and is computed using Equation (23).

$$Ey = -\Sigma_{k=1}^{255} P_k \log(P_k) \qquad (23)$$

The probability of occurrence of pixel value k is denoted by P_k. The value of $Ey \in [0, 8]$. For an 8-bit image, the entropy value should approach 8. Table 6 illustrates the entropy values of the chosen sample images, revealing that the entropy of all encrypted images closely approximates 8.



(a)

(b)

(c)

(d)

(e)

(f)

Figure 14. Pixel correlation analysis. (a) LCT_1. (b) $BMRI_1$. (c) $BMRI_2$. (d) CXR_1. (e) CXR_2 and (f) LCT_2.

Table 5. Differential attack analysis.

Image	NPCR	UACI
$BMRI_1$	99.59	33.61
$BMRI_2$	99.63	33.69
CXR_1	99.61	33.01
CXR_2	99.54	33.07
LCT_1	99.60	34.33
LCT_2	99.61	33.86

Table 6. Entropy analysis.

	Entropy	
Image	Original	Encrypted
$BMRI_1$	6.9816	7.9971
$BMRI_2$	6.9592	7.9969
CXR_1	7.6995	7.9969
CXR_2	7.6933	7.9970
LCT_1	6.2786	7.9970
LCT_2	6.9756	7.9969

5.9. *Error metrics*

There are few metrics available to assess the error of the encryption model. MAE, RMSE, and PSNR are standard metrics to assess whether the encryption scheme produces acceptable errors. MAE is used to measure the variance between encrypted and original images. MAE $\in [0, 2^m - 1]$, where m is the number of bits to represent each pixel. For a good encryption model, MAE should be

Table 7. Error metrics.

Image	MAE	RMSE	PSNR(dB)
$BMRI_1$	127.24	104.97	7.71
$BMRI_2$	127.46	105.07	7.70
CXR_1	127.33	103.13	7.86
CXR_2	127.98	103.28	7.85
LCT_1	127.30	107.14	7.53
LCT_2	127.62	105.72	7.65

maximum. It can be evaluated using Equation (24).

$$MAE = \frac{1}{\mathcal{W} \times \mathcal{H}} \Sigma_{p,q} \left|CMed(p,q) - Med(p,q)\right| \quad (24)$$

MSE is useful for comparing exact pixel values between an original image and an encrypted image. The error is the difference between the original image's and the encrypted image's pixel values. In order to provide more precise and reliable data, RMSE assesses the MSE root. A desirable encryption algorithm would yield a minimal RMSE value. Equations (25) and (26) can be used to calculate these measures.

$$MSE = \frac{1}{\mathcal{W} \times \mathcal{H}} \Sigma_{p,q} (CMed(p,q) - Med(p,q))^2 \quad (25)$$

$$RMSE = \sqrt{MSE} \quad (26)$$

The range of RMSE ∈ $[0, \infty]$. PSNR is used as a quality measurement between the original and decrypted images. PSNR is mathematically computed as follows in Equation (27).

$$PSNR = 10 \log_{10} \frac{(2^m - 1)^2}{MSE} \quad (27)$$

where m represents the number of bits per pixel. PSNR is measured in decibels (dB). Table 7 shows the error metrics of the sample medical images in the proposed model.

5.10. Known plaintext attack analysis

In the domain of image encryption, these assaults pose challenges, especially given the substantial data content typically found in images, making them complex targets for protection. Through these methods, adversaries aim to anticipate the link between plaintext and ciphertext images, seeking recurring patterns to deduce the secret encryption key or restore the original image. To counter known-plaintext attacks in image encryption, various plaintext images such as 'Black' and 'White' are selected as test subjects for encryption using the proposed QMedShield, as depicted in Figure 15, with the aim of undermining the scheme's integrity.

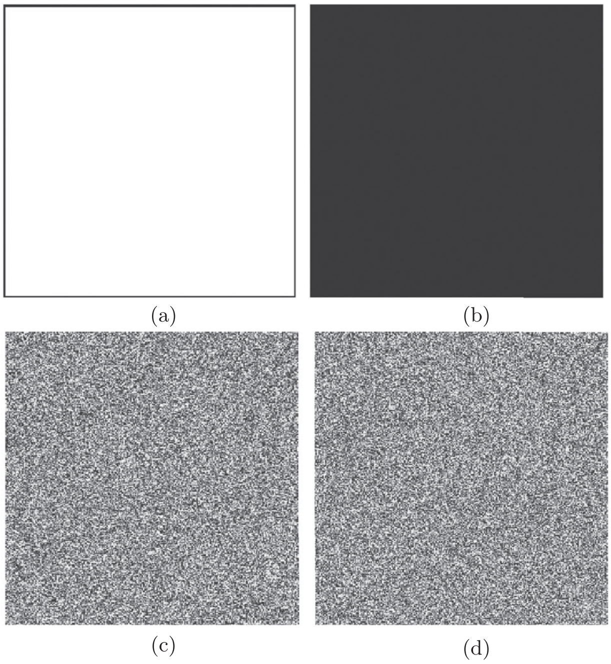


Figure 15. KP attack simulation. (a) White Image. (b) Black Image. (c) Encrypted White Image and (d) Encrypted Black Image.

5.11. Chosen plaintext attack analysis

Given that attackers exert greater influence over plaintext images, the chosen-plaintext attack holds more potency than the known-plaintext attack. Consequently, an image encryption algorithm capable of thwarting a chosen-plaintext attack is inherently resilient against a known-plaintext attack as well. To disperse pixel values effectively, QMedShield employs an XOR operation, while Equation (28) is utilized to assess its resistance against chosen-plaintext attacks.

$$Med_1(p,q) \oplus Med_2(p,q) = CMed_1(p,q) \oplus CMed_2(p,q) \quad (28)$$

In this scenario, Med_1 and Med_2 represent 2 test images and their respective encrypted cipher images are $CMed_1$ and $CMed_2$. If Equation (28) is fulfilled, then the CP attack is possible. The proposed method offers protection against such attacks, as illustrated in Figure 16, where Equation (28) is found to be unjustified.

5.12. Comparative analysis

The comparative analysis provided in Table 8 assesses the performance of the QMedShield encryption model against nine different existing image encryption schemes. Key metrics such as correlation coefficients in horizontal (Hcorr), vertical (VCorr), and diagonal (DCorr) directions, entropy, UACI, and NPCR are used to evaluate each model's effectiveness in securing image data.

Table 8. Encryption model: comparative analysis.

Reference	Hcorr	VCorr	DCorr	Entropy	UACI	NPCR
Zhou et al. [36]	0.0048	−0.0056	0.0028	7.9097	–	–
Liu et al. [38]	0.0002	0.0002	0.0005	–	33.44	99.68
Zhou et al. [28]	0.0006	−0.0101	0.0025	7.8958	–	–
Janani et al. [24]	−0.0045	0.0103	0.0011	–	33.46	99.72
Hu et al. [39]	−0.0021	0.0039	−0.0009	7.9968	33.46	99.60
Kiran et al. [40]	0.5421	0.5361	0.5078	7.9900	33.12	99.98
Amaithi Rajan et al. [22]	−0.0011	−0.0154	−0.0282	7.9971	33.39	99.61
Patel et al. [37]	0.0020	−0.0012	0.0043	7.9975	33.51	99.60
Mohamed Ihsan et al. [2]	0.0023	−0.0004	−0.0090	7.6434	33.63	99.60
QMedShield (Ours)	**−0.0347**	**−0.0211**	**−0.0418**	**7.9971**	**33.58**	**99.62**

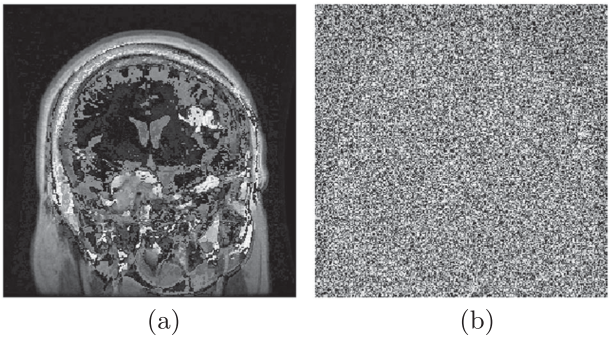


Figure 16. CP attack simulation. (a) $Med_1(p,q) \oplus Med_2(p,q)$ and (b) $CMed_1(p,q) \oplus CMed_2(p,q)$.

Correlation coefficients measure the linear relationship between adjacent pixels in encrypted images, which ideally should approach zero or negative values. Lower values indicate less correlation, meaning that the encryption scheme has effectively removed predictable relationships between neighbouring pixels. QMedShield is achieving values of −0.0347 (Hcorr), −0.0211 (VCorr), and −0.0418 (DCorr). These values are the lowest, indicating that QMedShield disrupts pixel correlations more effectively than other models. In comparison, Zhou et al. [36], and Patel et al. [37] achieve close to zero or slightly positive correlation values, which indicates some level of residual correlation between pixels. QMedShield's negative values in each direction demonstrate its robustness in pixel scrambling, providing a high level of pixel confusio,n which prevents statistical attacks.

Compared to other models, QMedShield achieves notably low correlation coefficients in all directions, showcasing its strong ability to obscure original image patterns. Its entropy value of 7.9971 approaches the ideal, indicating a high level of randomness. Moreover, QMedShield's UACI and NPCR values are comparable to or exceed those of other methods, confirming its strong resilience to attacks through excellent sensitivity and diffusion properties. Together, these results illustrate that QMedShield provides a robust encryption scheme that ensures high unpredictability, strong resistance to known attacks, and excellent sensitivity to input variations.

5.13. Theoretical security proof

This subsection theoretically proves that the proposed quantum-chaos-based image encryption scheme provides better security than traditional image encryption schemes.

Theorem 5.1: *Let Med_i be a grayscale medical image and $CMed_i$ be the ciphertext produced by the QMedShield encryption function $E_{QMedShield}(Med_i)$, which utilizes a combination of chaotic systems and quantum operations for encryption. The unpredictability and security of $CMed_i$ can be mathematically shown to exceed that of traditional encryption functions $E_{traditional}(Med_i)$ by demonstrating the enhanced sensitivity to initial conditions and the complex key generation process involved in the proposed algorithm.*

Proof: The encryption process of QMedShield begins with the generation of multiple keys from chaotic maps and quantum operations. The keys $K = \{k_1, k_2, k_3, \ldots, k_{18}\}$ are derived from the Henon map and a 3D quantum logistic map, which exhibit chaotic behaviour. The randomness and unpredictability introduced by these chaotic systems are characterized by the Lyapunov exponent λ. In our case, this leads to $\lambda_{QMedShield} > 0$, indicating that even a small perturbation in the initial parameters (e.g. k_1, k_2, k_3) significantly alters the output image $CMed_i$. This high sensitivity ensures that:

$$CMed_i(Med_i + \Delta Med) \neq CMed_i(Med_i) \tag{29}$$

where ΔMed is a small change in the input image.

Moreover, the encryption process involves the application of quantum gates (Hadamard and CNOT) on the scrambled image SI_i. This step introduces quantum superposition, whereby each pixel can exist in multiple states simultaneously. This can be expressed as $|\psi\rangle = \sum_{j=0}^{M-1} c_j |j\rangle$, where M is the number of possible states for each pixel. The superposition enhances the number of potential ciphertexts that can be generated from a single input image, leading to:

$$|CMed_i| \gg |C_{traditional}| \tag{30}$$

where $|CMed_i|$ and $|C_{traditional}|$ represent the size of the ciphertext spaces produced by the proposed and traditional methods, respectively.

Additionally, the chaotic diffusion keys K_X, K_Y, K_Z enhance the security of the encrypted image. The modulus operation ensures that the generated keys are uniformly distributed within the permissible range, preventing any predictable patterns in the output ciphertext. The combination of chaotic dynamics and quantum operations contributes to a high entropy measure $Ey(CMed_i)$, which can be represented as:

$$Ey(CMed_i) > Ey(C_{traditional}) \tag{31}$$

indicating greater randomness and making the ciphertext more resistant to cryptanalysis.

Thus, the rigorous mathematical framework established through the chaos-based key generation and quantum superposition illustrates that the QMedShield encryption model provides a significantly enhanced level of security and unpredictability over traditional encryption methods. ■

6. Conclusion and future works

With the exponential growth of medical imaging, robust encryption for secure cloud storage has become indispensable to protect sensitive patient information from potential cyber threats. This paper addresses the limitations of conventional and quantum-based encryption techniques in integrating with classical systems, particularly in resource-sensitive environments like healthcare. The proposed QMedShield encryption model combines quantum-inspired chaos, bit-plane scrambling, and DNA encoding within a hybrid framework, providing quantum-grade security while minimizing computational demands. By employing a quantum-chaos-based approach, QMedShield effectively balances security and resource efficiency, making it adaptable for classical systems that require high security without a full quantum infrastructure overhaul. This research contributes a practical, advanced encryption model capable of protecting medical images in cloud storage, demonstrating strong resistance to known attacks through rigorous theoretical and statistical validation. Looking ahead, future advancements could explore the application of high-dimensional quantum chaotic maps to further enhance pixel diffusion. Additionally, optimizing the storage of image pixels through efficient qubit-based pixel substitution holds promise. Moreover, the integration of scrambling techniques for both row and column pixels across each bit-plane could bolster the diffusion rate, contributing to the algorithm's overall security and effectiveness in securing sensitive medical imagery.

Acknowledgments

Conceptualization: Arun Amaithi Rajan, Vetriselvi Vetrian; **Methodology and Development:** Arun Amaithi Rajan, Vetriselvi Vetrian; **Formal analysis and investigation:** Arun Amaithi Rajan, Vetriselvi Vetrian; **Writing – original draft preparation:** Arun Amaithi Rajan, Vetriselvi Vetrian; **Writing – review, and editing:** Arun Amaithi Rajan, Vetriselvi Vetrian; **Supervision:** Vetriselvi Vetrian.

Data availability statement

The data underlying this article are derived from a source in the public domain. The sources are listed as follows:

(1) **Brain Tumor MRI Dataset** at https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset
(2) **Chest X-ray Dataset** at https://www.kaggle.com/datasets/nih-chest-xrays/data
(3) **Lung Cancer CT Dataset** at https://www.kaggle.com/datasets/adityamahimkar/iqothnccd-lung-cancer-dataset

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Arun Amaithi Rajan http://orcid.org/0000-0002-3019-5879
Vetriselvi Vetrian http://orcid.org/0000-0002-3832-6968

References

[1] Broz M. How many pictures are there (2024): Statistics, trends, and forecasts. 2024. https://photutorial.com/photos-statistics/.

[2] Mohamed Ihsan PM, Amaithi Rajan A, Vetriselvi V, et al. Qcrypt: advanced quantum-based image encryption for secure satellite data transmission. In: 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT); Trichirappalli, India: 2024. p. 1–9. doi: 10.1109/ICEEICT61591.2024.10718453

[3] Lovrenčić R, Škvorc D. Multi-cloud applications: data and code fragmentation for improved security. Int J Inf Secur. **2023**;22:713–721. doi: 10.1007/s10207-022-00658-8

[4] Liu Q, Zhou F, Chen H. Secure medical data on cloud storage via DNA homomorphic encryption technique. Phys Commun. **2024**;64:102295. doi: 10.1016/j.phycom.2024.102295

[5] Kaur M, Kumar V. A comprehensive review on image encryption techniques. Arch Comput Methods Eng. **2020**;27(1):15–43. doi: 10.1007/s11831-018-9298-8

[6] Yousif SF, Abboud AJ, Alhumaima RS. A new image encryption based on bit replacing, chaos and DNA

coding techniques. Multimed Tools Appl. **2022**;81(19): 27453–27493. doi: 10.1007/s11042-022-12762-x

[7] Xu G, Li H, Ren H, et al. DNA similarity search with access control over encrypted cloud data. IEEE Trans Cloud Comput. **2022**;10(2):1233–1252. doi: 10.1109/TCC.2020.2968893

[8] Zhou N, Chen W, Yan X, et al. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Inf Process. **2018**;17(6):137. doi: 10.1007/s11128-018-1902-1

[9] Wang L, Ran Q, Ma J. Double quantum color images encryption scheme based on dqrci. Multimed Tools Appl. **2019**;79(9–10):6661–6687. doi: 10.1007/s11042-019-08514-z

[10] Zhou N, Yan X, Liang H, et al. Multi-image encryption scheme based on quantum 3D arnold transform and scaled zhongtang chaotic system. Quantum Inf Process. **2018**;17(12):338. doi:10.1007/s11128-018-2104-6

[11] Zhou N-R, Wu J-W, Chen M-X, et al. A quantum image encryption and watermarking algorithm based on qdct and baker map. Int J Theor Phys. **2024**;63(4):100. doi:10.1007/s10773-024-05630-x

[12] Liu X-D, Chen Q-H, Zhao R-S, et al. Quantum image encryption algorithm based on four-dimensional chaos. Front Phys. **2024**;12. doi: 10.3389/fphy.2024.1230294

[13] Magdy M, Hosny KM, Ghali NI, et al. Security of medical images for telemedicine: a systematic review. Multimed Tools Appl. **2022**;81(18):25101–25145. doi: 10.1007/s11042-022-11956-7

[14] Priyanka, Singh AK. A survey of image encryption for healthcare applications. Evol Intell. **2022**;16:801–818. doi: 10.1007/s12065-021-00683-x

[15] Zhang Y, He Y, Zhang J, et al. Multiple digital image encryption algorithm based on chaos algorithm. Mob Netw Appl. **2022**;27:1349–1358. doi: 10.1007/s11036-022-01923-9

[16] Khare P, Srivastava VK. A secured and robust medical image watermarking approach for protecting integrity of medical images. Trans Emerg Telecommun Technol. **2021**;32(2):1–17. doi: 10.1002/ett.3918

[17] Tang J, Lu M, Zhang Z, et al. Novel asymmetrical color image encryption using 2D sine-power coupling map. Nonlinear Dyn. **2024**;112:11547–11569. doi: 10.1007/s11071-024-09644-2.

[18] Paul LSJ, Gracias C, Desai A, et al. A novel colour image encryption scheme using dynamic DNA coding, chaotic maps, and SHA-2. Multimed Tools Appl. **2022**;81:37873–37894. doi: 10.1007/s11042-022-13095-5

[19] Yi G, Cao Z. An algorithm of image encryption based on AES & rossler hyperchaotic modeling. Mob Netw Appl. **2023**. doi: 10.1007/s11036-023-02216-5

[20] Ahmad I, Shin S. Encryption-then-compression system for cloud-based medical image services. 2022. p. 30–33. doi: 10.1109/icoin53446.2022.9687214

[21] Arthi G, Thanikaiselvan V, Amirtharajan R. 4D hyperchaotic map and DNA encoding combined image encryption for secure communication. Multimed Tools Appl. **2022**;81:15859–15878. doi: 10.1007/s11042-022-12598-5

[22] Amaithi Rajan A, Vetrian V, Gladys A. Secure image encryption model for cloud-based healthcare storage using hyperchaos and DNA encoding. 2023. p. 89–103. doi: 10.1007/978-3-031-38296-3_8

[23] Abd El-Latif AA, Abd-El-Atty B, Talha M. Robust encryption of quantum medical images. IEEE Access. **2017**;6:1073–1081. doi: 10.1109/ACCESS.2017.2777869

[24] Janani T, Brindha M. A secure medical image transmission scheme aided by quantum representation. J Inf Secur Appl. **2021**;59(Apr):102832. doi: 10.1016/j.jisa.2021.102832

[25] Ma Y, Zhou N-R. Quantum color image compression and encryption algorithm based on fibonacci transform. Quantum Inf Process. **2023**;22(1):39. doi: 10.1007/s11128-022-03749-6

[26] Dai J-Y, Zhou N-R. Optimal quantum image encryption algorithm with the QPSO-BP neural network-based pseudo random number generator. Quantum Inf Process. **2023**;22(8):318. doi: 10.1007/s11128-023-04071-5

[27] Ran Q, Wang L, Ma J, et al. A quantum color image encryption scheme based on coupled hyper-chaotic lorenz system with three impulse injections. Quantum Inf Proces. **2018**;17(8):188. doi: 10.1007/s11128-018-1958-y

[28] Zhou N, Hu Y, Gong L, et al. Quantum image encryption scheme with iterative generalized arnold transforms and quantum image cycle shift operations. Quantum Inf Process. **2017**;16(6):164. doi: 10.1007/s11128-017-1612-0

[29] Houshmand M, Khorrampanah M, Alkhudhari AHM. Optimized quantum computing technique to encrypt medical images. Opt Quantum Electron. **2024**;56(3):442. doi: 10.1007/s11082-023-06041-8

[30] Kumar P, Rahman M, Namasudra S, et al. Enhancing security of medical images using deep learning, chaotic map, and hash table. Mob Netw Appl. **2023**. doi: 10.1007/s11036-023-02158-y

[31] Gao X, Liu X. CLSM-IEA: a novel cosine-logistic-sine map and its application in a new image encryption scheme. Signal Image Video Process. **2024**;18(4): 3063–3077. doi: 10.1007/s11760-023-02971-8

[32] Msoud Nickparvar. Brain tumor MRI dataset. 2021.

[33] Wang X, Peng Y, Lu L, et al. ChestX-ray8: hospital-scale chest X-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases. (Technical report). Available from: https://uts.nlm.nih.gov/metathesaurus.html.

[34] Nitha VR, Vinod Chandra SS. ExtRanFS: an automated lung cancer malignancy detection system using extremely randomized feature selector. Diagnostics. **2023**;13(13). doi: 10.3390/diagnostics13132206

[35] Wan Y, Gu S, Du B. A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy. **2020**;22(2):171. doi: 10.3390/e22020171

[36] Zhou NR, Hua TX, Gong LH, et al. Quantum image encryption based on generalized arnold transform and double random-phase encoding. Quantum Inf Process. **2015**;14(4):1193–1213. doi: 10.1007/s11128-015-0926-z

[37] Patel S, Thanikaiselvan V, Rearajan A. Secured quantum image communication using new two dimensional

chaotic map based encryption methods. Int J Theor Phys. **2024**;63(2):49. doi: 10.1007/s10773-024-05548-4

[38] Liu H, Jin C. A novel color image encryption algorithm based on quantum chaos sequence. 3D Res. **2017**;8(1):4. doi: 10.1007/s13319-016-0114-7

[39] Hu M, Li J, Di X. Quantum image encryption scheme based on 2D sin $e^2 - \mathit{logistic}$ chaotic map. Nonlinear Dyn. **2022**;111(3):2815–2839. doi: 10.1007/s11071-022-07942-1

[40] Kiran P, Parameshachari BD. Resource optimized selective image encryption of medical images using multiple chaotic systems. Microprocess Microsyst. **2022**;91:104546. doi: 10.1016/j.micpro.2022.104546