Journal of Information Security and Applications 59 (2021) 102832

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A secure medical image transmission scheme aided by quantum representation

T. Janani, M. Brindha *

Department of Computer Science and Engineering, National Institute of Technology, Tiruchirappalli, India

ARTICLE INFO

Keywords:
Quantum
Telemedicine
Chaos
Medical image
Encryption

ABSTRACT

Quantum information and quantum image processing have made immense progress in the most recent years. The proposed paper investigates the proficiency of quantum image encryption in the field of Telehealth which can be built by incorporating quantum block-based spatial transformations. The proposed quantum cryptosystem introduced two levels of security for medical image and its sensitive content. The secrecy of medical image is reinforced by choosing a plain image based initial seed values for encryption. It is found that the suggested quantum block-based scrambling can serve as a novel method for intensifying the privacy-preserving process of medical image. It additionally ensures the medical image integrity by introducing dedicated quantum encryption for ROI based regional data. With a bilateral image transmission perspective, the proposed paper introduced InterPlanetary Features based file system for proficient retrieval of medical images. The quantitative simulation and performance evaluation done on the Cancer Imaging Archive dataset manifests that the suggested quantum-based two-level security for medical images is suitable for reinforcing the confidentiality and privacy-preserving process. It also enlarges the effectiveness of quantum image processing applications in Telemedicine.

1. Introduction

Medicinal services and Information Technology have recently fascinated a lot of works in an affiliated manner which results in numerous changes in the medicinal domain. Telehealth is a data-centric clinical space where an immense amount of information is generated and accessed in a distributed cloud as a standard approach. In Telehealth, medical image processing is the predominant task where the treating and diagnosing of diseases can be done by sharing the images of X-ray, CT scan, MRIs and so on. Meanwhile, this ease of transmission increases data privacy and security issues as patient information moves around a distributed environment for storage and processing. For guaranteeing the secrecy and authentication of medical image data, cryptographic techniques are universally accepted in the bilateral transmission environment.

1.1. Background of the research

Over the past decades, broad investigations have been carried with the aspects of secure image transmission and retrieval techniques. Many schemes are proposed for securing the medical image by using chaotic maps at their pixel scrambling and diffusion stage [1–4]. Though these schemes ensure the randomization in the encryption, it may undergo classical attacks due to their fixed secret keys. To attain a secure and efficient keystream, Xingyuan W. et al. [5] proposed an LL compound chaos and ZigZag transform-based image encryption algorithm. Here, the advanced ZigZag transform and Lu system are jointly utilized for scrambling the input image whereas the composite chaotic system is used at the diffusion stage. The image sensitivity depends on local pixels which leads to minimal global entropy measures. Also, many one-time key based encryption schemes [6–8] are introduced for ensuring the resistance towards cryptanalytic attacks. H. Liu [6] presented a one-time-key cryptosystem using chaotic maps. For generating random sequences, author utilized MD5 based initial conditions and True Random Number Generator. Although the scheme has a very good key space using a low dimension chaotic map, it requires a large number of iterations for ensuring the divergence of the chaotic map.

Similarly, Mohamed Boussif [9] presented an adaptive block key for encrypting the medical image. Hua Z et al. [10] suggested high-speed pixel shuffling and adaptive diffusion-based medical image encryption by inserting random data into image for shuffling process. The reversible process is very tedious as it may lead to data loss during the image compression stage. B Abd-El-Atty [11] suggested Logistic-Chebyshev map based S-box and pseudo-random number generator for image encryption. By executing the combinational 1-D chaotic map, the

* Corresponding author.
E-mail addresses: saijanani.308@gmail.com (T. Janani), brindham@nitt.edu (M. Brindha).

https://doi.org/10.1016/j.jisa.2021.102832

Available online 26 April 2021

author generated a key image K for performing XOR operation over the original image. However, the scheme exhibits minimal UACI value than the proposed image encryption method.

To achieve high correlation on cipher images, many schemes are proposed for spatial permutation using high dimensional chaotic map [12–15]. Chen X. et al. [13] suggested an adaptive medical image processing depending on multiple chaotic mappings like logistic sine and hyper chaos. Boriga R et al. [14] presented a unique hyper-chaotic map using parametric conditions of the serpentine curve. H Liu suggested a bit-level permutation for encrypting the image based on PWLCM and Chen chaotic system [15]. Also, [16] presented an image encryption scheme by utilizing DNA complementary rule and chaotic map. The row and column permutation are carried out by using PWLCM and the resultant permuted image is encoded based on DNA complementary rule. Also, the initial conditions are based on applying MD5 over the input image. Similarly, [17] introduced a perceptron model-based image encryption scheme. But these methods results in a minimum Number of Pixel change Rate say 99.58, 99.5376, 76% [15–17] respectively also it has low key space when compared to the proposed quantum-based medical image encryption's NPCR and key space value. X Y Wang [18] suggested a DNA sequence operation based image encryption scheme. The scheme also utilized coupled map lattice for generating pseudo-random sequence which is later XOR-ed with the plain image in a bit-wise manner. To enhance the security level, the author utilized DNA matrix-based initial conditions for iterating a chaotic map. Also to resist the chosen-plaintext attack, [19] introduced a parallel image encryption algorithm using DNA encoding. The pixel reformations are performed with the help of random sequence generates by spatiotemporal chaos system.

There are also some data hiding methods were introduced for protecting the medical image sensitive data [20–22]. Parah, S. A et al. [20] recommended a high range reversible data hiding method for telehealth application. S. Das et al. [21] proposes a classical image watermarking technique using an ROI-lossless fragile technique. If the image has tampered, at that point it is unfeasible to recover the input image or sensitive data as there is no dedicated function for recovering the leaked data. Murali, P et al. [22] introduced copyright protection scheme for images which are outsourced in the third party database. Author ensures the prevention of unauthorized distribution of the images. Bouslimi, D et al. [23] suggested a hybrid encryption or watermarking scheme for preserving medical images. The time complexity is huge as it involves encrypting the watermarked image. Elhoseny, M., et al. [24] suggested a model for securing diagnostic data in the medical image by using steganography and hybrid encryption methods.

To optimize the efficiency of image encryption and to minimize the computational cost, X. Wang [25] recently presented a fast image encryption algorithm by combining cyclic shift and sorting operation for pixel permutation. The author introduced parallelism in the diffusion phase and achieved good randomness however the scheme exhibits less key space when compared to the proposed system which leads to the brute force attack. Dridi, M. et al. [26] recommended an image encryption method which depends on combined chaotic and neural networks. The complete image pixels are XORed with the chaotic keystream for shuffling and neural network model is applied for diffusion. Later, X. Wang [27] presented a study about the application of matrix Semi-Tensor Product for parallel updation of Boolean network encryption. Instead of using XOR operations during the diffusion phase, the author utilized different size of plaintext matrix to perform diffusion operation. Similarly, [28] suggested the Boolean network-based compound secret key generation for the image encryption process. The scheme achieves good security metrics by using semi-tensor products in the Boolean network. Yet it possesses minimal NPCR and UACI rate.

By utilizing the parallelism and network model, the algorithm exhibits better security metrics, but it might be vulnerable to cryptanalytic attack using high computation machines. With the agile improvement of calculations and the emergence of high computational workstations, the security of classical cryptography undergoes severe challenges like Shor factorizing algorithm which is the major threat for classical cryptosystems. Also, the introduction of Grover quantum search algorithm proved the powerfulness of quantum computing by reducing the complexity to $O(\sqrt{n})$. This evident the possibility of cracking classical cryptography using quantum machines. Indeed, well-structured security systems as listed in the literature might undergo quantum attack hence it is necessary to introduce a quantum resist cryptography technique to image security.

1.2. Previous related works on quantum cryptography and image retrieval

Recently, researchers have begun exploring the quantum-based image encryption methods for processing the sensitive data in a secure and efficient manner and as a result, efficient quantum chaos is introduced for image security [29–32]. To achieve high-security metrics on color image, Liu X. et al. [33] proposed a qubit rotation basis for encrypting the color images. The quantum converted image is randomly rotated quantum Fourier transform is applied for encrypting the image in the frequency domain. Liu, H et al. [34] suggested color image encryption using quantum chaos. To improve the secrecy of color image, the author utilized a two-dimensional logistic map and nearest neighboring coupled map. Similarly, XH Song [35] proposed restricted geometric and color transformations for scrambling the quantum image pixel positions. The encryption scheme depends on neighbor pixels, swapping and rotation angles. Though the encryption is performed in both spatial and frequency domains which gives a better security result, this scheme is applicable only for adjacent level qubit permutation.

For better pixel shuffling in quantum image, Liu X. et al. [36] suggested quantum image security by considering inter and intra bit permutation using logistic map. For medical image applications, Heidari, S., [37] suggested selective encryption for medical images. Author considers visually important area alone in the image and performs encryption on the same. Author claimed better time complexity as it encrypts the important region alone, it may lead to chosen ciphertext attack.

For establishing the non-linear dynamic behavior in secret key many schemes are proposed based on Quantum Walks [38–43]. AA Abd El-Latiff [38] presented a lightweight image encryption scheme by utilizing quantum walks as a random key generator. The suggested scheme uses quantum walks to construct permutation boxes for pixel confusion phase and PRNGs for the diffusion phase. However, the diffusion mechanism is invariant to plain text which may lead to chosen plaintext attack. AA Abd el-Latiff [39] introduced quantum walks and chaotic inducement-based substitution box (S-box) construction and they also suggested a bit-level cascaded quantum walk protocol for generating pseudo-random numbers. Similarly, B Abd-El-Atty [40] presented a one-particle quantum walk-based quantum image encryption. The randomness of quantum walks on a circle is utilized for the key generation process. Later the controlled not operation is introduced over the quantum image. However, these scheme exhibits a pixel change rate of 99.6% and 99.58% respectively which is less compared to the proposed scheme. To achieve high resistance towards the differential attack [41–43] utilized controlled alternate quantum walks (CAQW) for information security in the healthcare domain. The encryption mechanism in [43] depends on the controlled quantum walk which has two sorts of key parameters: one for permutation and another for substitution. Though it shows better computation speed, it possesses minimal NPCR and randomness when compared to proposed system. With the popularity of quantum-based image processing and its security measures, there exists some video encryption by adopting quantum cryptography. Song X.H et al. [44] proposed an encryption technique for videos by utilizing controlled XOR operations and logistic map. The system provides better results for each frame and the complexity depends on the frames. For hiding the sensitive data in quantum image, Abd EL-Latif et al. [45] introduced a quantum information

hiding technique such as quantum steganography in telehealth for concealing the secret data over the cover image. However, these bit-based embedding causes some pixel value changes in the cover image which may lead to guessing of the location of the watermark in the image. In a telehealth environment, images are circulated over distributed environment where user can upload and retrieve the images for diagnosing or consultation. Though there are efficient image encryption schemes which are listed in literature study, only few work has been carried out for secure and efficient retrieval. In order to retrieve the images efficiently from the cloud storage, the first searchable encryption was found by D. X. Song et al. [46]. With this continuation, many research work states about the efficient image retrieval from the cloud without disturbing the confidentiality of the images. Notably, C. Chang et al. [47] recommended a similar index for retrieving the encrypted data by computing the hash value. The existing searchable techniques are mostly centralized and suffers a single point of failure and additionally it consumes lot of time for searching the data.

By witnessing the above literature, the major problems in Telehealth environment and classical cryptography systems are: (i) Medical image confidentiality without loss of quality (ii) Preserving the trustworthiness of medical image's sensitive data i.e. Region of Interest data (iii) Efficient retrieval without decrypting the medical image in a distributed environment. (iv) Quantum resists cryptography scheme (v) differential attacks (vi) Robustness of secret key

1.3. Motivations of the research

In a Telehealth environment, medical images can be transmitted to any medical laboratories, medical practitioner, or specialist for consultation or referral cases. Generally, in a Telemedicine environment, image uploading and retrieval are the two crucial tasks because the medical image which is used for online consultation is very sensitive in nature and thus strict security measures should be taken for preserving these images. Also, it should guarantee the efficient and secure retrieval of the medical image to the query user. From these observations, it is clear that there are three factors to be analyzed for any medical image transmission method. (i) Privacy-preserving medical image (ii) Integrity of Region of Interest (tumor, injured area, MRI impression) of a medical image and (iii) secure retrieval of image for diagnosing. Many research works had been carried out for securing the medical image under cloud-based transmission but unfortunately, these works are focused on image confidentiality alone and not on the trustworthiness of ROI data and secure retrieval. Also, few shortcomings are reported such as computational overhead, resistance towards quantum cryptanalytic attacks, and adaptative behavior. So, this research work aims to develop a quantum resist secure medical image transmission scheme in which (i) medical images are encrypted using quantum cryptography (ii) the trustworthiness of the ROI data is preserved by introducing a dedicated ROI encryption phase (iii) Secure retrieval is achieved by incorporating InterPlanetary image Feature fie System where the medical image features are extracted and stored as a hashed values and later it is compared with user query image features. In other words, the main objective of the proposed scheme is to incorporate two levels of medical image security by utilizing basic quantum gates. To achieve this, a novel quantum block-based image scrambling is suggested for whole medical image and one-time pad encryption is proposed for ROI regional data. Thus, the principle contributions of the proposed paper are listed below:

1. The confidentiality of the medical image is preserved by introducing efficient block-based quantum image encryption using quantum spatial transformations.
2. Plain image based secret keys are employed for encrypting medical images to further enhance the security level.
3. The proposed system ensures the secrecy of ROI separately by encrypting the ROI boundary box value using quantum one-time pad encryption.
4. InterPlanetary Image Features file system is realized for efficient bilateral image transmission and retrieval under a distributed environment.
5. The proposed system guarantees both the secrecy and trustworthiness of the medical images in the telehealth environment.

The rest of this paper is organized as follows. Section 2 gives the preliminary work behind the proposed system. Section 3 discusses about the proposed encryption framework and the experimental analysis of the proposed system are carried out in Section 4. The comparison of the proposed methodology with state-of art methods are listed in Section 5 and Section 6 concludes the paper.

2. Preliminaries

The preliminary knowledge of the proposed framework includes the procedure involved in conventional system, quantum image representation and security threat model of the proposed system and the fundamental background of chaotic encryption scheme.

2.1. Hyper chaotic map

The proposed quantum encryption scheme utilizes chaotic maps for generating random sequences for permutation and diffusion. A hyperchaotic system is a chaotic system with more than one positive Lyapunov exponent which results high randomness on the space. Lorenz's hyper chaotic system is defined as

$$\begin{cases} X' = \sigma(Y_0 - X_0) + L_0 \\ Y' = X_0(\phi - Z_0) - Y_0 \\ Z' = (X_0 * Y_0) - (\alpha * Z_0) \\ L' = -(X_0 * Z_0) + (d * L_0) \end{cases} \tag{1}$$

Here X', Y', Z', L' are the time derivatives of the state variable X_0, Y_0, Z_0, L_0 with σ, ϕ, α as the system parameters and d is the control parameter. Hyper Lorenz chaotic system is more complex and the sequences are unpredictable, which results in strong resistance against adaptive argument synchronization attack. Each iteration of the hyper Lorenz produces four stochastic sequences which will act as a random key stream for permutation process.

2.2. Arnold map

The generalized two-dimensional Arnold chaotic map is expressed as

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \mod N \tag{2}$$

where, N is the size of the image, p and q are the control parameters. The Arnold chaotic map is used to create a quantum key image for diffusion process by converting it into Novel Enhanced Quantum Representation.

2.3. Novel Enhanced Quantum Representation (NEQR)

NEQR is the quantum grayscale representation where the original image pixel values are converted into their respective binary numbers and undergoes series of quantum operations. The first step is to prepare $q + 2n$ qubits, where n is the image size and the quantum gates are initialized with all zeros and identity gate is applied over it. The next step is to introduce the Hadamard gate for all the pixel coordinates. The image of size $M \times N$ is converted into q qubits where q is the range of grayscale. For a grayscale image I, the quantum representation NEQR is

$$|I\rangle = \frac{1}{2n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f(y,x)\rangle |YX\rangle \tag{3}$$

where $|f(y,x)\rangle$ is the pixel value and $|YX\rangle$ is the pixel position value. For each pixel, $q + 2n$ binary sequence is generated from the quantum circuit.

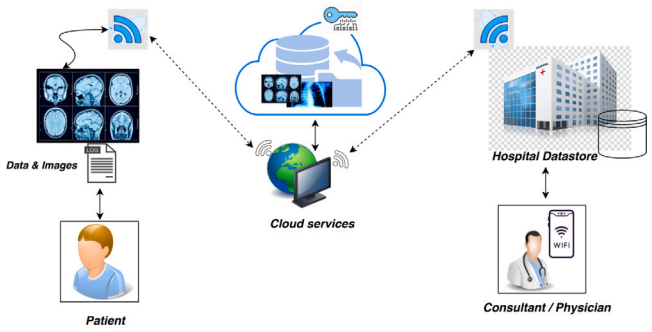

Fig. 1. Traditional system.

2.4. Conventional telehealth architecture

Fig. 1 shows the basic workflow of conventional Telehealth where the patients can remotely access the medicinal services like consultation, diagnosis, etc., from the physician. Also, Telehealth allows the physician to avail experts' opinions for their patients from different healthcare centers by sharing the medicinal reports. In conventional systems, patients or hospital jurisdiction can share the reports like data files or images of CT-scans, X-rays etc., to other parties by uploading it to the distributed platform. In this circumstance, the physician could diagnose the diseases remotely but it is open to numerous security risks. The primary risk factor in the conventional system is data privacy. Even though the image owner outsource the encrypted data to the distributed platform there is a gateway for intruders who can steal these sensitive data. Also, at the time of retrieval, the traditional system may exhibit single point searchable failure as the images are uploaded to the third-party database.

2.5. Security threat model

The conventional system solely depends on a third party database and it is assumed to be a trusted party. The medical images are uploaded in encrypted form and all computations like searching similar images, validating the integrity are done in the encrypted images which will increase the computational overload. Also, the medical images may exhibit two parts: Region of Interest (ROI) and Non-Region of Interest (NROI). The ROI region contains the most sensitive information, so it is necessary to preserve the image and as well as there is a requirement of additional protective shield for ROI.

3. Proposed architecture

To address the privacy issues in the conventional method, the proposed paper utilizes quantum cryptography in the Telehealth platform. The proposed framework ensures the data privacy and effective retrieval of medical images by introducing quantum block-based image encryption and distributed InterPlanetary Image Features File system for comparing the identical query image features. Fig. 2 depicts the proposed architecture for telehealth. As from Fig. 2, the proposed framework is divided into four stages: 1. Feature extraction 2. Quantum medical image encryption, 3. ROI regional data generation and encryption and 4. Medical image retrieval. For secure and efficient medical image processing, the image features are extracted and stored in the IPFS system. Meanwhile, the plain medical image endures two phases of security: 1. The ROI is extracted from the medical image with the help of boundary and the respective regional data is generated and encrypted using quantum one-time pad encryption technique. 2. The entire plain image is encrypted using a quantum block-based cryptographic technique. At the time of retrieval, query features are compared with the stored image features and the image integrity is checked by validating the regional data.

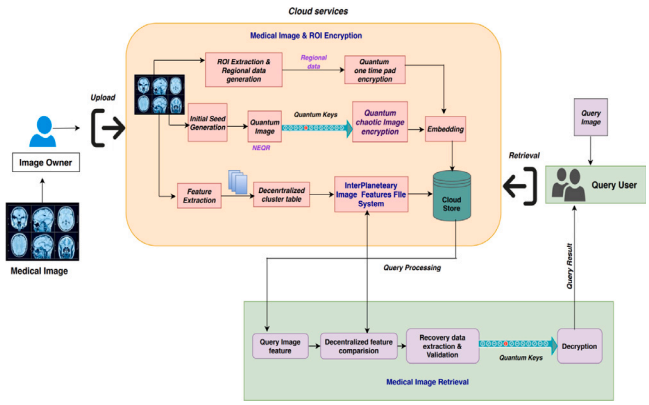

Fig. 2. Proposed architecture.

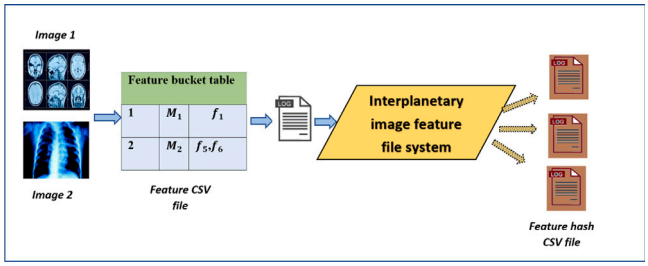

Fig. 3. Feature extraction.

Table 1
Feature bucket table.

S.No	Medical image ID	Cluster ID
1	M_1	f_1, f_4 f_{23} f_{17}
2	M_2	f_2, f_3 f_{41}
3	M_5	f_5, f_6

3.1. Interplanetary image features file system

The patient or hospital jurisdiction uploads the image to the distributed environment by extracting the plain image features and feature table is built. The proposed paper utilizes a Histogram of Gradient feature extractor and these extracted features are stored in a feature table. The intermediary server computes the features of a similar image and stores in a single bucket ie., clustered manner Table 1. shows the feature bucket table. Here, M_{id} denotes the id of the uploaded medical image similarly f_{id} shows the feature of the respective medical image. The entries of the cluster id consist of similar image feature say M_1, M_4, M_{23}, M_{17} features which are similar to the medical image M_1. At the time of retrieval, the query result depends on the feature comparison so it is necessary to preserve the image features as well. The features are crucial entries for identifying a similar image and it is stored as plaintext in a cloud server hence it is open for intruders to access it. To overcome this, the proposed paper utilized Interplanetary Image Feature File System for storing the image features. Fig. 3 shows the proposed workflow of medical image feature extraction. The feature bucket table entries are converted into csv files and these files are distributed in an IPFS server. The proposed system exhibits a secure feature comparison in the third-party database by utilizing IPFS.

3.2. Block-based quantum medical image encryption

The suggested framework employs quantum cryptography in Telehealth. The image owner/hospital authorities upload the image to the distributed environment for remote consultation or diagnosis. To

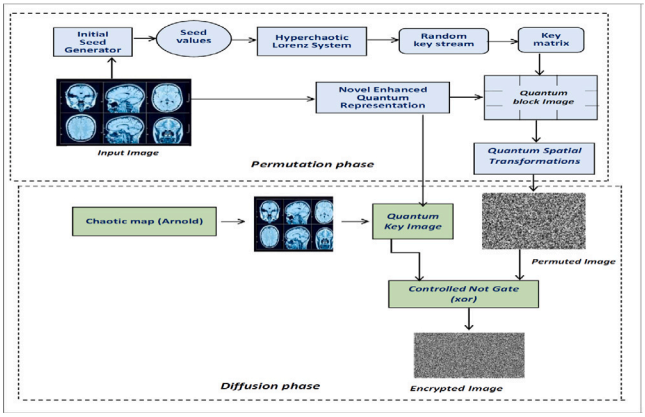

Fig. 4. Quantum block-based medical image encryption.

ensure the confidentiality of the outsourced data, the proposed paper introduces quantum chaos-based image encryption. First, the plain image based initial seeds are produced and utilized for random key sequence generation process in hyperchaotic Lorenz system. Then, inter and intra block permutations are employed for shuffling the pixel positions. Later, quantum-controlled image is constructed by iterating the Arnold chaotic map on original image. Next diffusion is performed by applying Controlled-NOT over quantum permuted and key image. Fig. 4 portrays the proposed quantum block image encryption. The proposed quantum block image encryption technique undergoes several steps and its explicit structure is given in Algorithm 1: Quantum block image encryption algorithm.

Algorithm 1: Quantum block image encryption

Input : Original Image I and Qubit key matrix K
Output: Encrypted Image I_{QEnc}
Call Initial_seed_generator ()
    Return seed values
Call Random_keystream_generator ()
    Return Qubit keystream matrix K
Construct quantum block image I_Q
    $|I_Q\rangle \Leftarrow NEQR[I]$
    Modified input image.
Call Inter and Intra Pixel reformations ()
    Matrix formations
Return I_Q^{st} : Perform Spatial transformations on I_Q
Call Quantum block Diffusion ()
    I^{AM} : obtain scrambled image.
    I_c : Obtain key image
Call CNOT.
Return encrypted image, I_{QEnc}

3.2.1. Initial seed generation

The proposed framework introduced a dynamic seed (initial condition) generation mechanism related to plain image for ensuring the randomness and sensitivity of proposed quantum cryptosystem. The work flow of the seed generation is shown in Fig. 5 and Algorithm 2: Initial seed generator dictates the steps involved in it. The proposed Initial_seed_generator () mechanism produces unique seed values for each image encryption as the procedure is highly related to plain image.

3.2.2. Random key stream generation

The spatial transformations or confusion phase is performed by generating random sequence from the chaotic map. The proposed

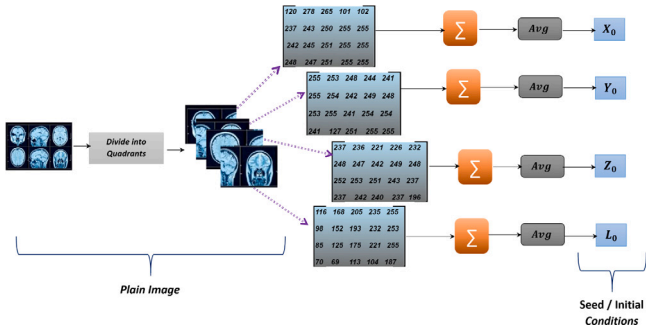

Fig. 5. Initial seed generation.

Algorithm 2: Initial Seed Generator

Input : Plain Image I
Output: X_0, Y_0, Z_0, L_0
Procure the Plain image I of size $N \times N$
check the size of image, *dim*
if $dim = N \times N$ **then**
    Divide I into $N/4$ blocks
    for $(i,j) in N/4$ **do**
        Read the pixel at I in a matrix form and compute

$$X_0 = \frac{\sum_{i,j=1}^{N/4} I(i,j)}{n}$$

    end
    end
else
    Divide I into $M/2$ and $N/2$ blocks and compute

$$X_0 = \frac{\sum_{i=1}^{M/2} \sum_{j=1}^{N/2} I(i,j)}{n}$$

end Repeat step 2 and 3 for calculating Y_0, Z_0, L_0.

framework utilizes high dimensional hyperchaotic Lorenz map for generating random keystream sequence. The high dimensional chaotic framework has more positive Lyapunov exponent which results a good dynamic characteristic. The Algorithm 3: Random keystream generator shows that random qubit keystream is generated by utilizing the seed values as from Section 3.2.1 and control parameters as $\sigma = 10, \phi = 8/3, \alpha = 28$ and $d = 2$. The chaotic characteristics of the adopted hyperchaotic Lorenz system with chosen initial seeds are given in Fig. 6. From the phase portraits given in Fig. 6, it is shown that, the hyperchaotic 4dimensional Lorenz system exhibits the property of randomness under the given initial values and it is chosen to design the proposed cryptosystem. Its higher degree of chaotic nature has made it suitable tool for incorporating secure communication. The chaotic map is fed with the initial seed values and iterates for n times, for each iteration it results four chaotic sequence X', Y', Z', L' and convert it into integer sequence with the upper bound of 256. Next, the quantum key streams are generated by converting the values into binary numbers where qubit $\in 0, 1$ and tensor product is applied to the resultant binary value as

$$|x \otimes y\rangle = |K_{x1}\rangle, |K_{x2}\rangle ... |K_{xn}\rangle \otimes |K_{y1}\rangle |K_{y2}\rangle |K_{yn}\rangle \quad (4)$$

The element $X \otimes Y$ will be viewed as a vector in a new vector space which carries the description of the quantum states of the system of two sequence. This $\otimes$ operation is called the tensor product. The tensor

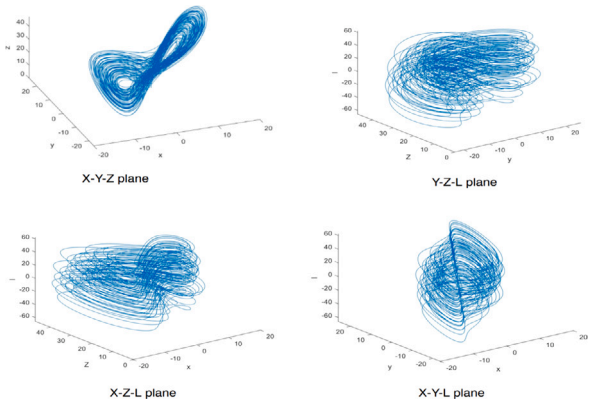

Fig. 6. Hyperchaotic Lorenz -Chaotic attractor with proposed initial seed when $\alpha = (24, 30]$ (a) projection on x-y-z plane (b) projection on Y-Z-L plane (c) projection on X-Z-L plane, (d) Projection on X-Y-L plane.

product of two sequence yields the key matrix as

$$Qubitkeymatrix \quad k = \begin{pmatrix} |K_{x1}\rangle, |K_{y1}\rangle & |K_{x1}\rangle, |K_{y2}\rangle & .. & |K_{x1}\rangle, |K_{yn}\rangle \\ .. & .. & .. & \\ |K_{x1}\rangle, |K_{y1}\rangle & |K_{x1}\rangle, |K_{y2}\rangle & .. & |K_{x1}\rangle, |K_{yn}\rangle \end{pmatrix} \tag{5}$$

Algorithm 3: Random Keystream Generator

Input : X_0, Y_0, Z_0, L_0 and control parameters
Output: Qubit key matrix $|k\rangle$
1 Set initial seed and control parameters
for $i = 0 to N$ **do**
Calculate chaotic stream X', Y', Z', L' as

$$X' = \sigma(Y_0 - X_0) + L_0; \qquad Y' = X_0(\phi - Z_0) - Y_0$$

$$Z' = (X_0 * Y_0) - (\alpha * Z_0); \qquad L' = -(X_0 * Z_0) + (d * L_0)$$

end
2 Generate integer sequence $X = (X_0)_{i=0}^{N-1}$ by applying $mod 256$
3 Repeat 2 for remaining chaotic sequences
4 Construct qubit key sequence $|K\rangle$
Transform entries of integer sequence X, Y, Z, L into 8-bit binary qubits
Apply Tensor product on X, Y as in Eq.4
Qubit keystream matrix K

3.2.3. Quantum representation

The original image I is converted into quantum Image for importing the quantum operations on it. The quantum image is prepared using Novel Enhanced Quantum Representation (NEQR) and it act as a input image for proposed quantum block based medical image encryption. The sample image block is shown in Fig. 7. For each pixel value, $|I\rangle = \frac{1}{2n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|f(y,x)\rangle|YX\rangle$ is computed and its representations are shown in Fig. 8.

After this representation, blocks are identified from the quantum image I_Q. To achieve high randomness in encryption, the proposed system maps the random blocks to the space for performing block-level spatial transformations.

3.2.4. Inter and intra pixel reformation

The spatial transformations or confusion phase is accompanied by two steps: inter block scrambling and intra block scrambling. Scrambling is used to shuffle the pixel values within and among the subsequent NEQR blocks. The Algorithm 4: depicts the steps involved in proposed Inter and Intra pixel reformation phase. The scrambling

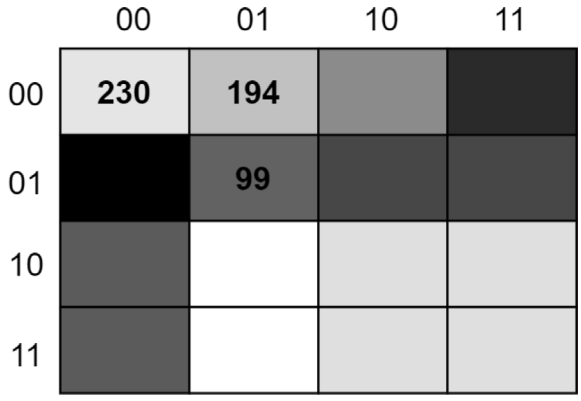

Fig. 7. Quantum grayscale image block with pixel values.

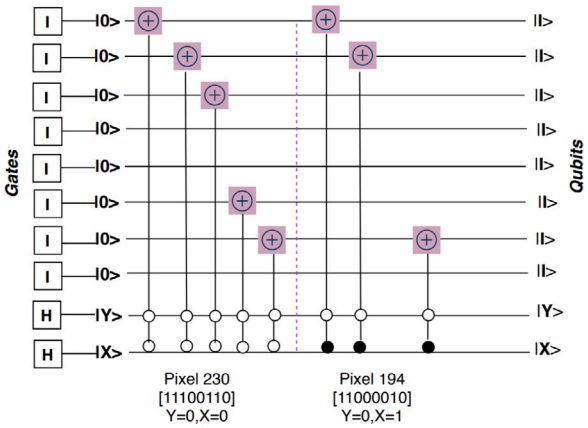

Fig. 8. Quantum circuit for representation.

operations for inter block permutations are pixel scrambling, qubit rotations, matrix transpose and row–column shuffling with rotation angle.

Algorithm 4: Inter and Intra pixel reformations

Input : Qubit key matrix $|k\rangle$ and Quantum image I_Q
Output: Image I_Q^{st}
// Pixel reformations
for (i, j) *in* I_Q **do**
Reform the pixel position using $|K\rangle$
Obtain I_{QP}
end
foreach $2^{(k-1)} \times 2^{(k-1)}$ *sub-blocks in* I_{QP} **do**
Map I_{QP} for spatial transformations
$(I_{(2^{(k-1)})})^{pp} \Leftarrow (I_{(2^{(k-1)})})^{\circ}$
foreach *row in* I_{QP} **do**
Perform $n/2$ rotation
end
foreach *column in* I_{QP} **do**
Perform $n/2$ rotation
end
perform $(I_{(2^{(k-1)})})^T \Longleftarrow I_{(2^{(k-1)})}$
end
Return I_Q^{st}

The first step in confusion phase is to scramble the image pixels according to the keystream matrix. The quantum block image is taken as an input and applied in the scrambling procedure. The proposed quantum encryption employs a scrambling procedure with the help of

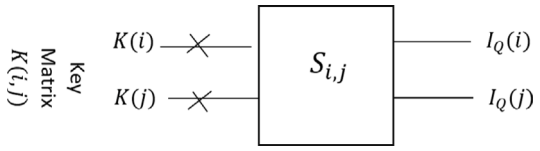

Fig. 9. Swap gate for pixel reformations.

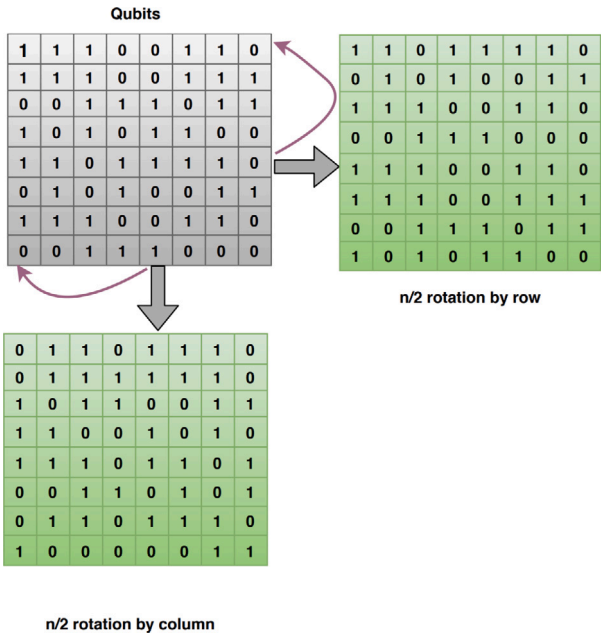

Fig. 10. Qubits rotations.

hyperchaotic sequence. The key sequences generated in Section 3.2.2 undergoes quantum tensor product operation ⊗ and produce key matrix of size $n \times n$. According to key matrix in Eq. (5), the quantum image undergoes pixel reformations. Specifically, the entries (i, j) in K represents the pixel positions of the image. The value in $K(i, j)$ replaced the value at the position (i, j) in the new image. The swap gate $S_{(i,j)}$ for the pixel reformations is shown in Fig. 9. For ensuring more randomness, the proposed encryption scheme incorporates qubit rotation in the scrambled image matrix. The sample qubit rotations are given in Fig. 10 where the qubits are rotated in both row and column manner with the rotation of $n/2$. Once the qubits are rotated, the pixel matrix undergoes row–column shuffling process with the rotation angle of 180° and finally permuted image I_Q^{st} is obtained by taking transpose.

3.2.5. Quantum block diffusion

For diffusing the pixel values, the quantum key image is generated by using Arnold chaotic map over the original image. Algorithm 5: Quantum block diffusion gives the steps involved in diffusion process. From NEQR representation, the size of the pixel value is $q + 2n$ which exhibits the number of key rounds k for Arnold map and thus the base image is generated. The obtained base image is converted into the quantum image as given in Section 3 for incorporating the quantum operations on it. Once the images are converted, controlled – NOT quantum gate is utilized for producing the encrypted image by coupling the scrambled block image obtained from Section 3.2.4 with a quantum base image.

3.3. ROI regional data encryption and embedding

To authenticate the trustworthiness of outsourced medical image, the suggested system introduced ROI based regional data encryption.

Algorithm 5: Quantum block Diffusion

Input : Image I_Q^{st} and Initial Conditions
Output: Encrypted Image I_{QEnc}
// Key image for diffusion
foreach *pixel* (i, j) *in original image* **do**
  Iterate Arnold map k rounds obtain I^{AM}
  Obtain Key image $[I_c] \Leftarrow NEQR[I^{AM}]$
end
foreach *pixel in* I_Q^{st} *and* $[I_c]$ **do**
  Apply quantum CNOT
end
$I_{QEnc} \Longleftarrow$ reshape I_{cnot}

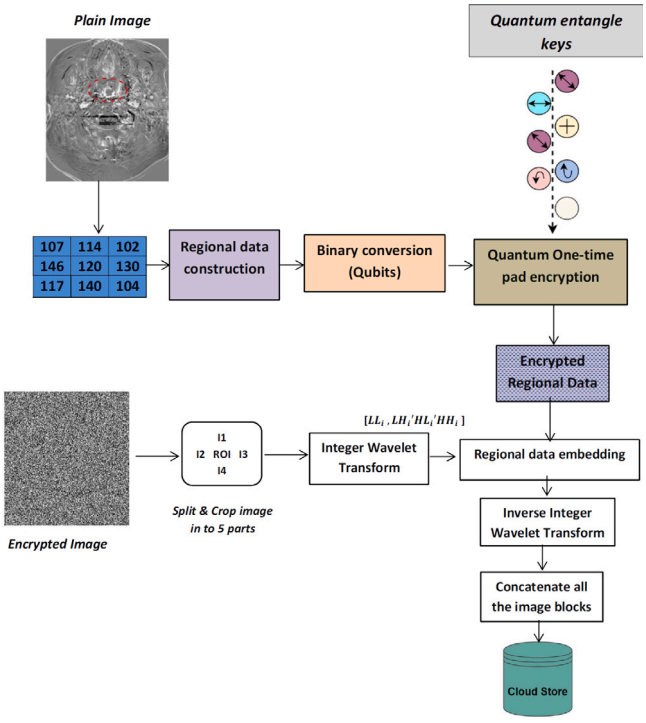

Fig. 11. Regional data encryption and embedding.

In medical image processing, Region of Interest (ROI) is the area that holds more sensitive content say boundaries of a tumor, injured area, etc. Thus, preserving the ROI contents is more important in the telehealth domain. Fig. 11 shows the steps involved in regional data encryption and embedding. While outsourcing the image, the proposed framework allows the image owner/hospital jurisdiction to mention the ROI boundaries for later extraction process. With the specified boundary value, the proposed system extracts the ROI and generates the stream of pixel difference value called regional data. The regional data is generated as

$$R_X = P_{i+1,j+1} - Pij \tag{6}$$

where, P_{ij} is the pixel values within ROI boundary. In existing methods, regional data is simply embedded with the image for validation. Yet this is open to intruders who can extract the data and gain knowledge about the ROI content from the image. Thus, it is important to encrypt the regional data too. To achieve this, the proposed system utilizes quantum one-time pad encryption for preserving the regional data. The proposed algorithm for encrypting ROI regional data is given in ROI encryption algorithm. As the algorithm depicts, the regional data is generated from the pixel difference and it is converted into qubits.

These qubits are entangled and angles are measured and denoted as a key for encryption. After obtaining the key, the proposed paper utilizes quantum-controlled gates over key values and qubits. This yields the encrypted regional data and it is inserted to the RONI region of the encrypted image. For embedding the encrypted regional data into a cover image, the proposed paper utilizes reversible watermarking depending on the standard Integer wavelet transform method (IWT). The image is subdivided into four parts concerning to ROI i.e., left, right, top and bottom. For each subblock, the lower and higher frequency sub-bands are identified with the help of IWT. Upon identifying the frequency band, the regional data is embedded as a reversible watermarking protocol. Similarly, frequency bands for other subblocks are identified and the complete regional data is embedded in the RONI part.

Algorithm 6: ROI encryption

Input : ROI Regional data R
Output: Embedded image with encrypted ROI R_{Enc}.
// Extract ROI
for *ROI boundary values* **do**
  Read the pixel values
  if *pixel value is not multiples of 3* **then**
    Take pixel from nearby RONI
  end
end
//Regional data generation
foreach *pixel* (i, j) *in ROI* **do**
  $R_X = P_{(i+1,j+1)} - P_{ij}$
end
//Regional data Encryption
  R_q ; convert R_X into binary qubits
  Measure quantum entangles, q_e among qubits and record it.
  $K \Longleftarrow q_e$
  $R_{Enc} = R_q Cnot K$
Embeds R_{Enc} in lower sub bands

3.4. Medical image retrieval

Medical data uploading and retrieval are two common tasks in the Telemedicine environment. The proposed paper employs the quantum encryption technique as a data preserving strategy while outsourcing sensitive data to the third-party database. Similarly, at the other end of the proposed framework, a query user or physician or another health care center retrieves a similar image or data by uploading the query. Fig. 12 shows the steps involved in proposed medical image retrieval scheme. In the proposed system, the query user can submit the query image to the service provider who can extract the query features and send them to the IPFS server. The server converts the query feature into hashed value and compares it with the stored hash values. Upon matching, the server returns the id of similar images to the service provider which results in the set of similar encrypted images. After validating the query user, the service provider performs quantum image decryption as in Algorithm 7. Once the images are decrypted, the integrity of medical images are validated by extracting the regional data from the image using its boundary value. The same procedure is carried out for generating the new ROI regional data which is in encrypted form. For decrypting the regional data, the server measures the qubit entanglement and obtains the key for decrypting the regional data. The same process is continued for each qubit i.e., for 8 rotations. After 8 rotations, the decryption process would be carried out where query user measures all the qubit encrypted value and record it for obtaining the final value. Hence, for verifying whether the ROI data has tampered or not, authenticated query users will record each qubit measurements in the ROI data and verifies with the original data.

Algorithm 7: Medical Image Retrieval

Input : Query image Q_I
Output: Original Image I
Perform feature extraction on query image
call Interplanetary image features file system
call Quantum image decryption ()
foreach *pixels* (i, j) *in* I_{Enc} **do**
  Iterate Arnold map k rounds
  Generate base image , I_c
  Obtain scrambled image
  $I_Q^{st} = I_c Cnot I_{Enc}$
end
foreach $2^{(k-1)} \times 2^{(k-1)}$ *block in* I_Q^{st} **do**
  Perform Inverse spatial transformation
  Obtain normalized quantum image I_Q
end
Result set of similar plain images
Extract Regional data $R_d^{'}$
Perform quantum measurement I
Quantum deciphered $R_d^{'}$
Compare with actual regional data R_d
if $(R_d^{'} = R_d)$ **then**
  Return image to user
else
  Image altered, notifies user and image owner

After comparison, if the regional data mismatches, then it indicates that the ROI has been tampered and notification is sent to the image owner otherwise the trustworthiness of the image has been preserved and the respective plain image is transmitted to the user.

4. Results and performance discussion of the proposed scheme

On account of the present condition, that the physical quantum machines are not available, the proposed medical image and ROI encryption techniques are assessed by utilizing IBM Quantum Experience and also simulated in a individual workstation with subsequent characteristics: MATLAB R 2019a, Windows 10 64-bit, Intel Core i7, with RAM of 16 GB memory. The time and complexity are the important factors considered for evaluating the suggested medical image and ROI encryption. To examine the proposed method for security and robustness, the simulation is carried out on different medical images from The Cancer Imaging Archive (TCIA) dataset composing of CT-scan images, Mammograms, MRI, and X-rays along with additional standard medical images. Note that, the images are used for the experiment after resizing it all to 512×512 pixel gray scale values.

4.1. Performance of medical image encryption

The proposed framework uses TCIA images for simulation. The sample images are depicted in Fig. 13(a) along with their respective quantum images in Fig. 13(b). At this stage, quantum image will act as an input for the proposed framework and inter and intra block permutations were carried out. The intermediate result of spatial transformations is given in Fig. 13(c). Meanwhile, the framework generates a key image by using quantum chaotic map say Arnold map. The key image is utilized for encrypting the medical image and the respective encrypted image is presented in Fig. 13(d).

4.1.1. Key space analysis

Key space is an important criterion for an efficient encryption algorithm to resist against exhaustive attack. The brute force attack is directly related to the key space hence a desirable encryption scheme

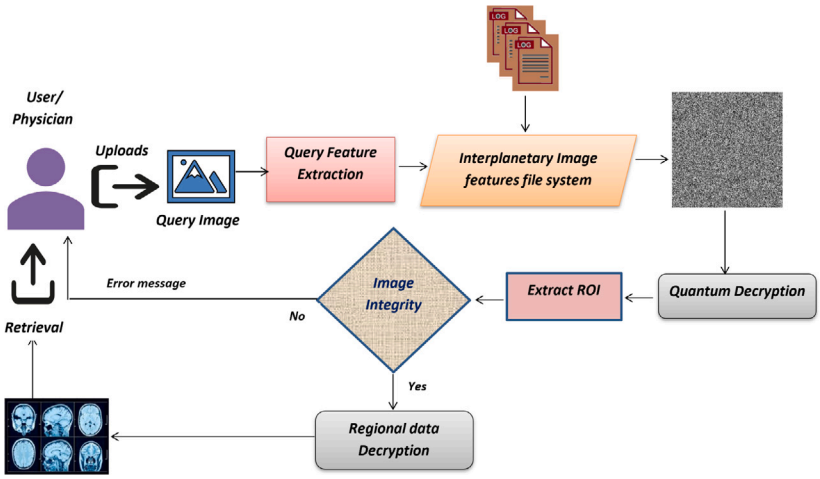

Fig. 12. Medical image retrieval.

should possess large key space. The proposed system utilizes four initial seed values X_0, Y_0, Z_0, L_0 for pixel reformations with control parameters σ, ϕ, α and d. Also, the proposed scheme exhibits a and b as an initial condition for diffusion process with control parameter p and q. According to the IEEE floating point standard [26], 10^{-15} is the computational precision of the 64−bit double-precision. By considering the computational precision (7), the proposed scheme exhibits a key space of $10^{180} \approx 2^{600}$ which is sufficiently large enough to make exhaustive attacks infeasible.

$$key = 10^{(-15)(12)} = 10^{180} \approx 2^{600} \tag{7}$$

4.1.2. Key sensitivity analysis

An ideal encryption scheme is key-sensitive where a small change in the key will cause a significant change in output [48]. Thus secrecy of the proposed system depends upon initial seeds of the chaotic map which in turn relies on plain image pixel values. Hence the sensitivity of the proposed system is tested by changing any one of keystream values and maintain others unchanged. The following steps are carried out for performing key sensitivity analysis.

1. The initial conditions x_0, y_0, z_0, l_0 are fed into the chaotic system and iterates up to n times which produce Qubit key matrix $|K\rangle$.
2. The original image I is encrypted using Qubit key matrix $|K\rangle$ and the resultant image is I_{QEnc}.
3. Then, a small deviation as incrementing and decrementing the keys by 10^{-15} is given to the proposed encryption scheme and the respective cipher image are I^{+}_{QEnc} and I^{-}_{QEnc}.
4. Also, key values of Arnold cat map a and b is increased by 0.00000000010 and utilized for decryption.
5. Now the mathematical analysis for the key sensitivity is performed by calculating the difference rate between I_{QEnc}, I^{+}_{QEnc} *and* I^{-}_{QEnc} with the help of (8) and the values are tabulated in Table 2.

$$D(K) = \frac{\sum_{i=0}^{x-1}\sum_{j=0}^{y-1} \Delta(I_{QEnc}(i,j), I^{+}_{QEnc}(i,j)) + \Delta(I_{QEnc}(i,j), I^{-}_{QEnc}(i,j))}{2 \times x \times y} \times 100 \tag{8}$$

where x and y are the sizes of the image and $\delta(A, B)$ be the difference rate of two cipher image A and B which can be determined by the following conditions:

$$\Delta(A,B) = \begin{cases} 1; if\ A(i,j) \neq B(i,j) \\ 0; if\ A(i,j) = B(i,j) \end{cases} \tag{9}$$

Table 2
Difference $D(K)$ under various key values.

Keys	Chaotic map	Value	Increment	$D(K)$
x_0	Hyper chaotic Lorenz	6.79925×10^{-11}	10^{-15}	99.7213
y_0		5.20135×10^{-11}	10^{-15}	99.7211
z_0		2.28982×10^{-11}	10^{-15}	99.7156
l_0		0.28915×10^{-11}	10^{-15}	99.7089
a	Arnold	0.698315687	10^{-15}	99.7402
b		0.227649743	10^{-15}	99.7398

From the table, it is clearly shown that there exists a strong sensitivity towards the initial conditions hence a small deviation in the key values results huge difference rate between ciphered images. The above procedure is analyzed visually by taking the plain MRI image and encrypted using the Qubit key matrix using actual initial conditions and modified initial conditions as shown in Fig. 14. Here, Fig. 14(a) shows the original medical image and encrypted with the actual key which results Fig. 14(b). Fig. 14(c) shows the decrypted image with key value as $x_0 = 6.79925 \times 10^{-11}$ and Fig. 14(d) shows the decrypted image with key value as $y_0 = 5.2898210\times^{-11}$. From the figures, it is evident that keys with minor changes cannot decrypt the images properly.

4.1.3. Plaintext sensitivity analysis

In addition to key sensitivity, plaintext sensitivity also a significant criterion to assess the effectiveness of a proposed image encryption algorithm. In other words, the encryption scheme should be very sensitive to the plain image in accordance with the one-bit change. The proposed system uses plain image related keys for encryption i.e., it uses plain image related initial conditions for iterating the chaotic map whose resultant sequence is used for pixel confusion phase. Additionally, to enhance the security level, the proposed scheme introduces plaintext related key image $|I_c\rangle$ to perform diffusion over a permuted image. The $|I_c\rangle$ is a quantum representation of input image where one-bit difference causes significant changes in the key image. The plaintext sensitivity is quantitatively evaluated by using NPCR, UACI metric and their analysis are given below:

A. Study of differential attack. A wise encryption scheme must resist towards differential attacks i.e., the recommended scheme needs to be responsive to the small changes in input image. Generally, two standard evaluation metrics are utilized for analyzing the effect of pixel shifts in the input image under the encrypted image. By [49], the metrics are number of pixels change rate (NPCR) and unified average change intensity (UACI) and it is formulated as

$$NPCR = \frac{\sum_{(x=1)}^{a}\sum_{(y=1)}^{b} D(x,y)}{(a \times b)} \times 100\% \tag{10}$$

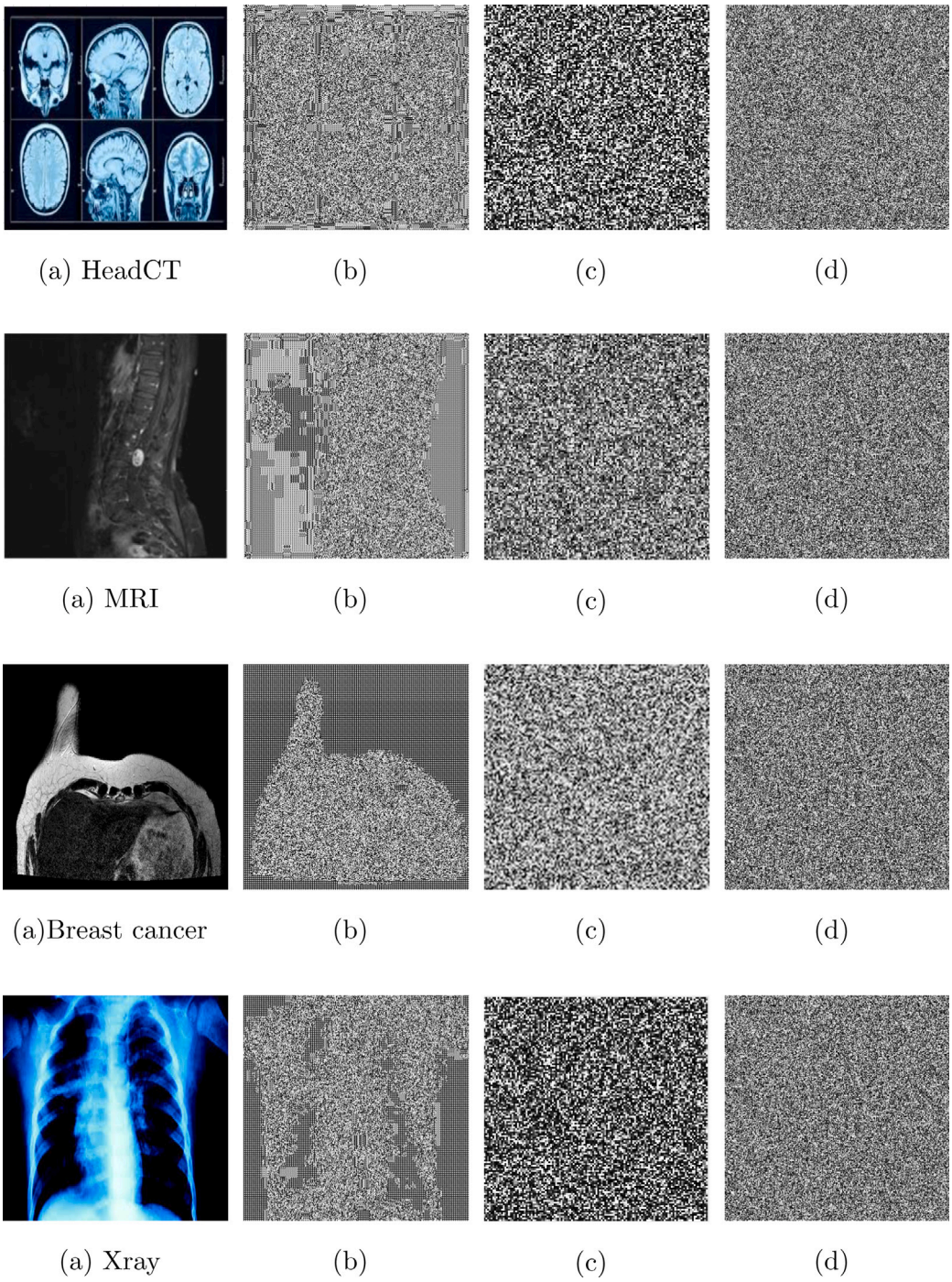

Fig. 13. Proposed Quantum block based encryption(a) plain images, (b) Quantum input images (c) Quantum image spatial transformations and (d) Encrypted image.

where,

$$D(x,y) = \begin{cases} 0, if\, e_1^{(x,y)} = e_2^{(x,y)} \\ 1; otherwise \end{cases} \tag{11}$$

here e_1 and e_2 are the cipher images whose original images are differed by one pixel and $a \times b$ is size of the image.

UACI is expressed by:

$$UACI = \frac{1}{(a \times b)} \sum xy \frac{|e_1(x,y) - e_2(x,y)|}{255} \times 100\% \tag{12}$$

The standard CT scan image is considered for examining the performance of proposed scheme towards differential attacks. The result analysis shows that, the single pixel value difference in plain image exhibit 99.78% NPCR and 33.47% UACI which implies that the suggested scheme is more sensitive to original medical image. Table 3 dictates NPCR and UACI esteems with different medical images. Also, the secret key of the proposed quantum block-based encryption technique is related to the image itself. Hence the proposed scheme makes a better performance for data privacy in telehealth field.

B. Avalanche effect. A better encryption method should result a highly sensitive encrypted image to changes in plain image pixel values. The proposed framework includes a dedicated module for plain image based initial seed generation which results different cipher whenever the

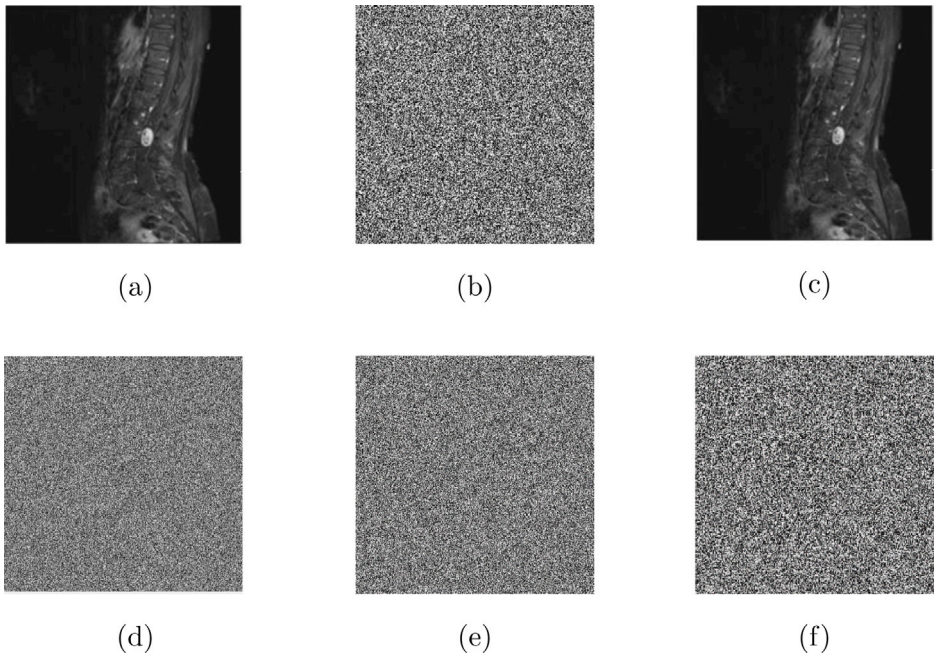

Fig. 14. Key sensitivity test. (a) original image, (b) encrypted with correct key (c) decrypted image (d) decrypted image with modified $K(i, j)$, (e) decrypted image with one bit change in chaotic sequence (f) decrypted image with different a and b.

Table 3
NPCR and UACI metrics for proposed encrypted images.

S.No	Image	NPCR	UACI
1	Head CT	99.7852	33.4762
2	Left arm X-ray	99.7685	33.201
3	Chest	99.7793	33.989
4	Spine MRI	99.7684	33.326
5	Brain MRI tumor	99.7987	33.4021
6	CT scan breast cancer	99.7889	33.4523
7	Mammography 1	99.7669	33.498
8	Abdomen CT	99.6923	33.3921
9	Head CT 2	99.6972	33.4376
10	Brain MRI 2	99.8472	33.4421
11	Spine MRI - axial	98.8973	33.4012
12	Left arm X-ray	99.7683	33.396
13	X-ray 2	99.7987	33.387
14	Coronary calcium scan 1	99.6978	33.498
15	Coronary calcium scan 2	99.7834	33.468
Average		**99.7172**	**33.4511**

Table 4
Avalanche effect on proposed quantum encryption scheme.

Plain image trial (pixels altered randomly)	Modified seed values (as per plain image)	Difference (original and new cipher)
Head CT	X_0 = 6.881371386718753 Y_0 =5.886138916015625 Z_0= 6.292657407031252 L_0 = 5.965495489843741	99.7852
Left arm X-ray	X_0 = 7.235677209123315 Y_0 =6.984322096510364 Z_0= 6.6678902655147828 L_0 = 6.225689126729390	99.7685
CT scan breast cancer	X_0=8.992367891022001 Y_0 = 8.776923650912674 Z_0= 6.2378946901120843 L_0=8.001276234560823	99.7889

plain image gets modified. Table 4 shows the different trials of plain image with pixel modification and its difference rate.

Table 5
Information entropy for proposed scheme.

S.No	Image	Entropy
1	Head CT	7.9968
2	Left arm X-ray	7.9902
3	Chest	7.9923
4	Spine MRI	7.9854
5	Brain MRI tumor	7.9813
6	CT scan breast cancer	7.8999
7	Mammography 1	7.9676
8	Abdomen CT	7.8975
9	Head CT 2	7.9958
10	Brain MRI 2	7.9850
11	Spine MRI - axial	7.9961
12	Left arm X-ray	7.9965
13	X-ray 2	7.9962
14	Coronary calcium scan 1	7.9983
15	Coronary calcium scan 2	7.9945
Average		**7.978227**

4.1.4. Randomness test analysis

The proposed scheme is tested for randomness by utilizing information entropy metrics. The entropy is the common tool to quantify the strength of encryption algorithm in a randomness perspective. The entropy $H(s)$ is given by

$$H(S) = \sum P(S_i) log \frac{1}{p(S_i)} \tag{13}$$

Table 5 shows that the average value of the proposed encryption method and it is nearer to the standard value 8. The above formulae for Information entropy depict the global randomness. The proposed quantum block-based encryption scheme utilizes inter and intra block spatial transformation, so it is necessary to measure the randomness with respect to local blocks. The local Shannon entropy is given as

$$\overline{H_{k,T_B}(S)} = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{14}$$

where, (S_i) are the blocks and T_B is the pixel. The experiment is carried out with the same set of medical images. The quantum images are split

Table 6
Histogram variances with respect to a secret key of the proposed algorithm.

Test cipher image	$\|K\rangle$	$\|K_1\rangle$	σ	ϕ	α	d
Head CT	261.927	275.236	269.896	247.245	260.298	266.476
Left arm	254.326	269.672	259.754	262.964	247.286	244.485

in to 16 blocks and these are examined for local randomness among the selected blocks. The average local entropy value for all the blocks in the ciphered head CT image is 7.9024 which is nearer to the standard value. This experimental outcome depicts that the proposed quantum block image encryption method achieves high randomness and secure against cryptanalytic attack.

4.1.5. Histogram study

The image histogram intuitively reflects the dissemination of grayscale values. To resist the statistical attacks, the cipher image should possess uniformity in grayscale distribution. This can be evaluated with the help of plotting the histograms for the cipher image. Fig. 15 presents the histogram of the input image and the respective encrypted image. From the figure, it is clear that the histograms of the proposed encrypted images are closely uniform and shows notable changes from the input image histogram.

Besides, variance analysis is carried out as a quantitative measure of each key with respect to histogram property. The smaller variance value indicates the better uniformity of the encrypted image [50]. Thus, the variance of the histogram is analyzed with respect to the change in the encryption key and it is expressed as

$$Var(H) = \frac{1}{m^2}\sum_{p=1}^{m}\sum_{q=1}^{m}\frac{(h_p - h_q)^2}{2} \tag{15}$$

where h_p and h_q represents the number of gray value pixels, m denotes the total number of gray values and the outcome H vector set of histograms. Table 6 exhibits the variances of the histograms of different ciphered images obtained by the proposed encryption scheme under different secret keys and parameters. The first column represents the variance values obtained by using the initial key matrix $|K\rangle$ while those variances in the following columns are obtained by changing any one of the secret parameters. From Table 6, it is clearly shown that the values of the variance of cipher images fall under the range of 250–270, which indicates the average fluctuations of the number of pixels in each gray value are about 14 pixels. However, the quantitative measure of variance for the histogram plain Head CT is 37425.00267 which is far greater than the variance of cipher image. Hence, the proposed encryption mechanism can withstand any statistical attack.

4.1.6. Chi-square test

The histogram plots provide the visual representation of pixel value distribution in cipher images whose uniformity demonstrates the effectiveness of the proposed encryption scheme towards the statistical attack. In addition to visual representation, the chi-square test is utilized as a quantitative metric for analyzing the uniformity of histograms. The mathematical expression for the Chi-square test is given in (16).

$$\chi^2 = \sum_{j=0}^{255}\frac{(A_i - P_i)^2}{P_i} \tag{16}$$

Where, P_i is the predicted frequency of pixel rate on the histogram of a ciphered image which can be obtained by $\frac{(M\times N)}{256}$, where $M \times N$ is the size of the test image and A_i is the actual frequency of pixel value j. An encryption scheme is said to be effective if it possesses a less observed chi-square value when compared to the theoretical value. Table 7 depicts the outcome of Chi-square analysis under the significance level of $\alpha = 0.05$ with the theoretical value 293 and the proposed system qualifies the chi-square test and indicates uniform distribution of pixel value in cipher images.

Table 7
Chi-square analysis.

Image	Size	χ^2	Result $\chi^2_{255,0.05}$
Head CT	256 × 256	261.268	Pass
MRI	256 × 256	254.326	Pass
CT-Breast	256 × 256	229.476	Pass
X-ray	256 × 256	285.385	Pass
Mammography 1	256 × 256	234.541	Pass
Abdomen CT	256 × 256	287.430	Pass
Head CT 2	256 × 256	290.110	Pass

Table 8
Correlation coefficients.

S.No	Encrypted image	Horizontal	Vertical	Diagonal
1	Head CT	−0.0025	0.0039	−0.0189
2	Left arm X-ray	0.0211	0.0314	0.0196
3	Chest	−0.0137	0.0225	0.0321
4	Spine MRI	0.0112	0.0245	0.0483
5	Brain MRI tumor	−0.0019	−0.0102	0.0131
6	CT scan breast cancer	0.0167	0.0235	−0.0018
7	Mammography 1	0.0021	0.0256	0.0235
8	Abdomen CT	0.0103	−0.0034	0.0029
9	Head CT 2	−0.0051	0.0063	0.0189
10	Brain MRI 2	−0.0067	−0.0014	0.0075
11	Spine MRI - axial	0.0017	0.00187	0.0015
12	Left arm X-ray	0.0014	−0.0052	0.0039
13	X-ray 2	−0.0187	0.0165	0.0025
14	Coronary calcium scan 1	−0.08761	0.0073	−0.0018
15	Coronary calcium scan 2	0.0048	0.0084	0.0012
Average		**−0.00446**	**0.0103**	**0.00106**

4.1.7. Correlation study

An appropriate encryption scheme ought to create an encrypted image with less correlation among the adjacent pixels. The image correlation between any two adjacency pixels can be measured as an important metric for evaluating the encryption process. The following equation is utilized to evaluate the correlations between adjacent pixels of the proposed encrypted image.

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{(V(x)V(y))}} \tag{17}$$

where $E(x)$ and $V(x)$ are the Expectation and Variance respectively. The analysis is carried out by randomly selecting 1000 adjacent pixel pairs from the plain and encrypted image and the values are tabulated in Table 8. The outcomes show that the correlation among the pixels are nearly zero in the encrypted image. Fig. 16. gives the correlation plots of adjacent pixels in cipher image in which Fig. 16(a), (b), (c) depict the horizontal, vertical and diagonal correlation of the encrypted image respectively. It delineates that the arbitrarily chosen pixels on the encrypted images are weakly correlated which demonstrates the effectiveness of proposed quantum block-based encryption scheme.

4.1.8. Resistance to noise attack

In a cloud-based data sharing environment, the cipher image is exposed to all sorts of noises. An ideal image encryption scheme should minimize the noise effect during transmission. Thus, to examine the efficiency of the proposed system towards the noise resistance, a test image of size 256 × 256 is taken and exposed to Gaussian noise with different variance values. Fig. 17(a-c) indicates the ciphered image which is exposed to different variants of Gaussian attack and its corresponding decrypted images are shown in Fig. 17(d-f). From Fig. 17, it is clearly shown that, even though the encrypted image is exposed to Gaussian noise, the decrypted image of the proposed scheme holds most of the original data. This guarantees the resistance towards noise attack.

4.1.9. Time complexity

The time complexity of the proposed cryptosystem is evaluated in terms of time consumed for performing quantum block based image encryption and regional data encryption.

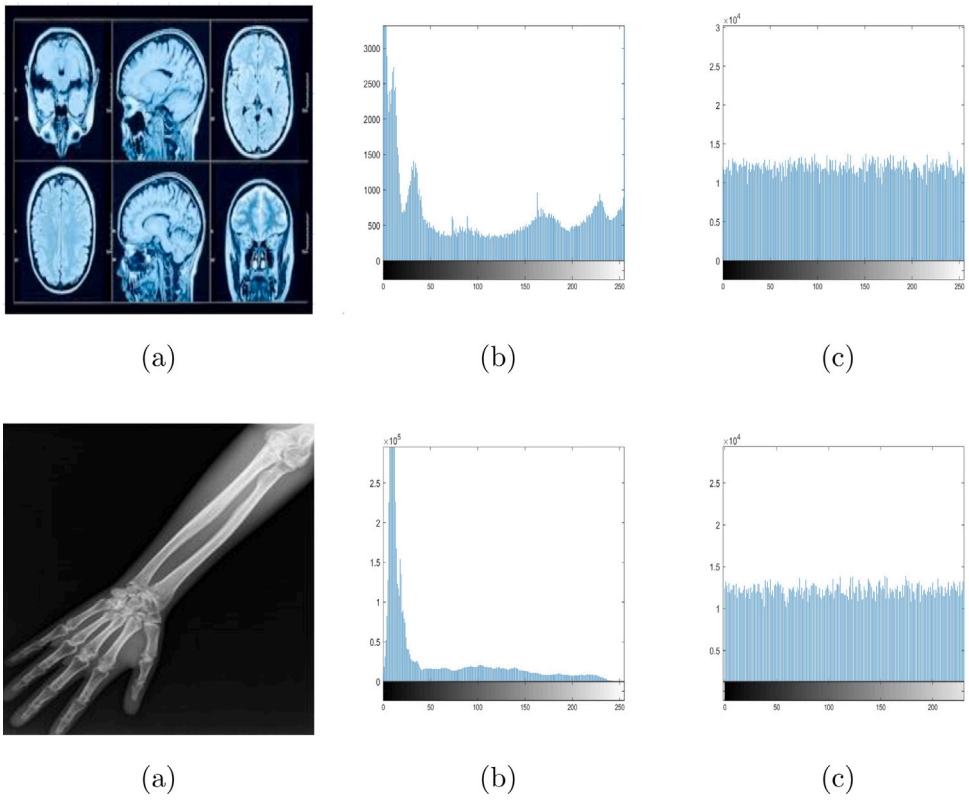

Fig. 15. Histogram analysis. (a) Plain Image, (b) histogram of plain image, (c) histogram of cipher image.

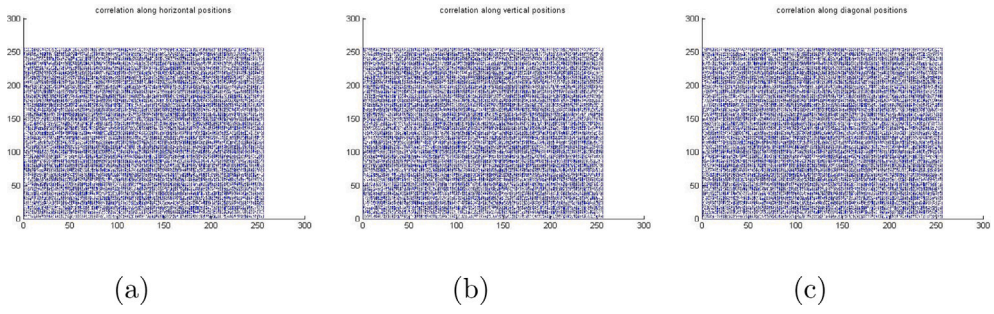

Fig. 16. Correlation analysis. (a) Horizontal correlation, (b) vertical correlation, (c) Diagonal correlation.

Table 9
Time complexity of proposed encryption.

S.No	Image size	Encryption time (s)	Decryption time (s)
1	64 × 64	0.023	0.0156
2	128 × 128	0.197	0.145
3	256 × 256	1.42	1.21
4	512 × 512	1.76	1.54

Table 10
Time complexity of proposed regional data generation and embedding.

S.No	Image size	ROI size	Regional data size	Regional data generation (s)	Embedding time (s)	Extraction time (s)
1	128 × 128	48 × 48	12 567	0.4135	0.4126	0.391
2	256 × 256	90 × 90	27 382	0.7539	0.8934	0.9923
3	380 × 430	45 × 45	19 452	0.3945	0.5189	0.5289
4	512 × 460	120 × 120	42 107	1.2367	1.5621	1.754

A. Speed analysis of proposed quantum block based encryption. The important factor for evaluating the performance of any encryption algorithm is said to be speed metrics. Table 9 shows the time complexity of the suggested quantum image encryption and decryption algorithm with different sizes which that the suggested algorithm is fast enough for adopting it in practical applications.

B. Speed analysis of regional data extraction and watermarking. The proposed regional data encryption for preserving the medical image integrity is carried out in sample medical images with different modalities and size. The images with different ROI regional data with time complexities are listed in Table 10. These outcomes demonstrate that the proposed techniques outperform efficiently in terms of speed and resistance towards the attacks.

4.1.10. Computational complexity

The computational complexity of the proposed quantum block-based medical image encryption depends on the number of basic logic elements such as CNOT and NOT and Toffoli gates which is utilized for the encryption process. Specifically, the complexity of the proposed scheme depends on XOR, shift and swap operations. According to the

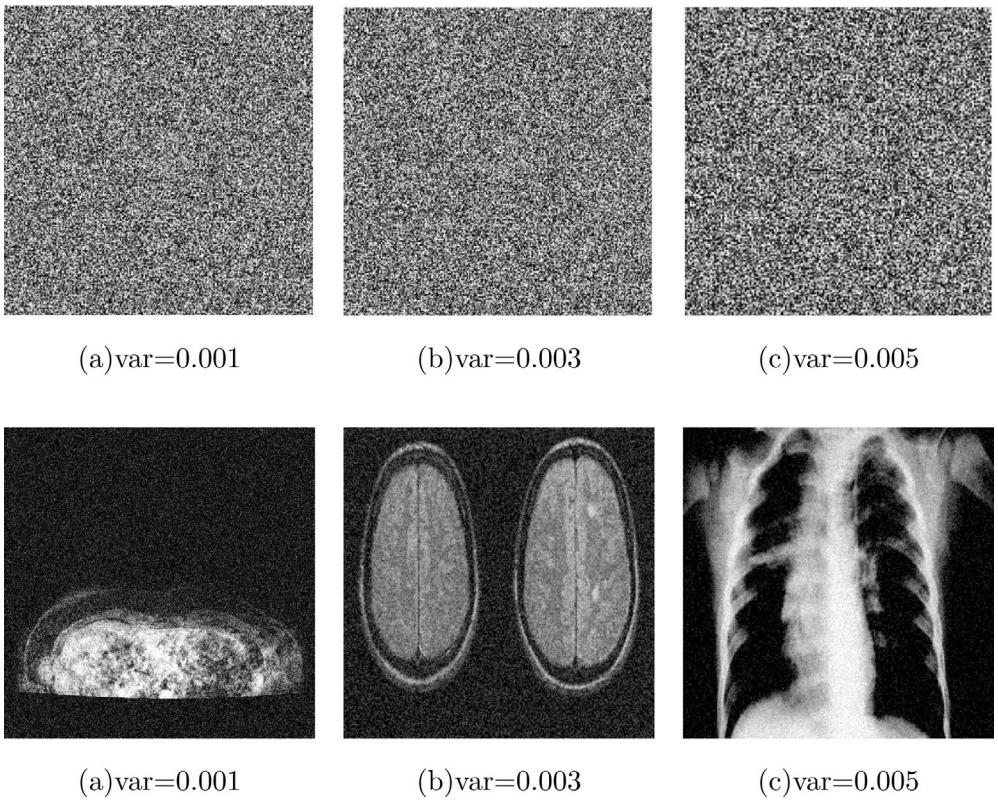

Fig. 17. Encrypted and decrypted images under different Gaussian noise levels with mean value = 0.

Fig. 18. Swap gate implementation using basic gate.

parallel characteristics of quantum computation, the grayscale information of each pixel in the quantum image is processed by the XOR operation, which is realized by $2n - CNOT$ gate. It is understood that n-CNOT gate is equivalent to $(2n-1)$ Toffoli gates and one CNOT, where one Toffoli gate can be simulated by using six controlled gates. Consider an image of size $2^n \times 2^n$, the computational complexity of the proposed system is given below:

A. Proposed quantum medical image encryption. A medical image of size $2^n \times 2^n$ undergoes proposed quantum block-based image encryption which is accompanied by the following operations. First, the quantum image goes through the pixel confusion stage i.e., pixel processing, pixel scrambling, and qubit orthogonal rotations. The proposed system utilizes a swap gate for pixel reformations with the key image as a controlled condition and this can be simulated with the help of three CNOT gates. Fig. 18 shows the implementation of the swap gate which can be simulated using three CNOT gate with the complexity of $O(3N)$. Next, qubit orthogonal rotations of about angle 90° is performed with the complexity of $O(n)$. Once pixel positions are reformed, the scrambled image is diffused by using CNOT over Arnold quantum key image and permuted image. The quantum XOR operation i.e., CNOT requires 128–256 basic gates. Thus, the computational load for CNOT gate is $O(N)$.

B. Proposed ROI regional data encryption. To authenticate the integrity of medical image sensitive data, the proposed system introduced ROI regional data encryption. The regional data generation is composed of data generation with the complexity of $O(N)$ followed by qubit conversion $O(N)$ then controlled XOR operation applied over quantum keys and regional data whose complexity is $O(N)$. Table 11 shows the overall complexity of the proposed quantum medial image encryption. By analyzing the complexity of the proposed system in classical computers, it requires two- 2 input multiplexers and one XOR gate for implementing one controlled swap gate. The complexity of multiplexers and XOR gate is $O(2^{2N} + N + 2^{2N})$. Similarly, the complexity for performing orthogonal rotations in the classical computer is $O(2^{2N})$. Therefore, the proposed quantum-based medical image encryption scheme take advantage over its conventional counterparts with respect to computational complexity.

Table 11
Computational complexity of each operation in proposed system.

S.NO	Operation	Complexity
1	Quantum medical image encryption	
	Pixel reformations	$O(3N)$
	Orthogonal rotations	$O(N)$
	Controlled XOR	$O(N)$
2	ROI regional data encryption	
	Regional data generation	$O(N)$
	Qubit conversion	$O(N)$
	Controlled XOR	$O(N)$
	Total	$O(8N)$

4.1.11. Ability to resist classical attacks

When an attacker meets the cipher image in cyberspace, he mainly targets to reveal the intermediate parameters rather than secret key parameters. Refs. [51,52] listed several challenges for protecting the image in cyberspace. By addressing these challenges, the proposed image encryption scheme focuses on the Telehealth application scenario with two levels of security i.e., block-based quantum image encryption

for medical image and ROI pixel value encryption for ensuring medical image sensitivity. In general, cryptanalyst uses the knowledge about the workflow of cryptosystem and tries to perform decryption of different cipher image by extracting their secret parameters.

An ideal and efficient cryptosystem should resist the cryptanalytic attacks through which an attacker can interrupt any sort of cryptosystem by utilizing different types of attacks: ciphertext only, known plaintext, chosen ciphertext and chosen plaintext attack [53].

Ciphertext only attack: The attacker has no other supplementary information except the intercepted ciphertext. They analyze the intercepted cipher image and extract its pattern or information string to reveal the plain image or secret key. Yet extracting a pattern or information from ciphertext alone is a difficult task.

Known-plaintext attack: The intruder maintains information regarding plain image and its respective cipher image and tries to disseminate the secret key.

Chosen ciphertext attack: The intruder may access the decryption cryptosystem temporarily and choose a cipher image randomly to perform decryption operation and obtain its relevant plain image.

Chosen plaintext attack: The intruder may temporarily access the encryption cryptosystem and randomly choose some set of plain images to generate the corresponding cipher image and targets to reveal the keys or original plain images. Many researchers have contemplated that some cryptosystem can be successfully cracked by known/chosen-plaintext attack [51–55].

Known/chosen plaintext attack. Among different types of classical attacks, the known/chosen-plaintext attack is most vulnerable since the attacker analysis the plaintext and their respective ciphertext and deduce some intermediate parameter (or) pattern to recover the secret keys. In the proposed system, the intermediate parameters can be obtained by choosing a random plain image with a different pixel value distribution pattern. Consider, the image in the proposed framework is represented as a matrix of size $N \times N$, where N is the size of the image, the pixel reformation is represented as (18).

$$I_Q^{st} = |K\rangle |I_Q\rangle \tag{18}$$

Where, $|K\rangle$ is the secret qubit transformation matrix generated from a chaotic map. Later, the key image $|I_c\rangle$ is XORed with the shuffled image I_Q^{st} by using a controlled CNOT gate as (19).

$$I_{QEnc} = |I_Q\rangle CNOT I_Q^{st} \tag{19}$$

By investigating (18) and (19), the attacker will try to realize the permutation pattern through which a plain image can be easily retrieved. In general, attacker chooses random images of size $N \times N$ with sequential pattern of pixel values i.e., $\begin{pmatrix} 1 & \ldots & n-2 & n \\ .. & .. & .. & .. \\ n & .. & n-2 & n \end{pmatrix}$ and access the encryption machinery to obtain corresponding permuted image. For simplicity, attacker may choose following combination of input images to retrieve the secret intermediate parameter say permutation pattern or diffusion keys. Let us consider, quantum input matrices as: I_{Qi} and tries different scrambling operations to obtain the intermediate permutation matrix I_{Qi}^{st}.

1. Sample image with identical row values

$$I_{Q1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 \end{bmatrix}; \; I_{Q1}^{st} = \begin{bmatrix} 3 & 3 & 1 & 1 \\ 4 & 4 & 2 & 2 \\ 1 & 1 & 3 & 3 \\ 2 & 2 & 4 & 4 \end{bmatrix};$$ obtained pixel pattern be p_1.

2. Sample image with identical column values

$$I_{Q2} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix}; \; I_{Q2}^{st} = \begin{bmatrix} 4 & 4 & 4 & 4 \\ 3 & 3 & 3 & 3 \\ 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 1 \end{bmatrix};$$ pixel pattern be p_2

Table 12
Known/chosen plaintext attack - log.

S.No	Plain image	Resultant permuted image	Pixel reformation pattern
1	I_{Q1}	I_{Q1}^{st}	$I_{Q1}(r_{11}, r_{12}, r_{13}, r_{14})$= $I_{Q1}^{st}(r_{31}, r_{32}, r_{13}, r_{14})$
2	I_{Q2}	I_{Q2}^{st}	$I_{Q2}(r_{11}, r_{12}, r_{13}, r_{14})$= $I_{Q2}^{st}(c_{41}, c_{42}, c_{43}, c_{44})$
3	I_{Q1}	I_{Q1}^{st}	$r_3 \Leftrightarrow r_1$

3. Image Random pixel values

$$I_{Q3} = \begin{bmatrix} 230 & 194 & 90 & 160 \\ 185 & 70 & 120 & 99 \\ 213 & 60 & 213 & 190 \\ 156 & 28 & 0 & 80 \end{bmatrix}; \; I_{Q3}^{st} = \begin{bmatrix} 213 & 60 & 213 & 190 \\ 185 & 70 & 120 & 99 \\ 230 & 194 & 90 & 160 \\ 156 & 28 & 0 & 80 \end{bmatrix};$$

p_3

By analyzing the sample input matrix and its respective permutation matrix, attacker maintains a log for different input cases as shown in Table 12 for obtaining plain image where P_i shows, the relationship between the sample input images and permuted images. Utilizing these logs information, attacker may rearrange the original permutation matrix for accessing the original input image.

To overcome this, and to achieve a high resistance towards cryptanalytic attack, the uncertainty principle of quantum mechanics is utilized in the proposed system for designing quantum controlled basic gates. These controlled gates are used for generating plain image related quantum key matrixC, key image $|I_c\rangle$ and quantum secret keys for performing the adaptive permutation and diffusion process. The dynamic qubit key matrix $|K\rangle$ is designed by employing high dimensional hyperchaotic Lorenz map where the initial conditions are associated with the plain image. Later, the random sequences are converted into quantum vectors by using controlled basic gates and the tensor product is applied over any two sequences of size $(1 \times N)$ and $(1 \times N)$ which results in a key matrix $|K\rangle$ of size $N \times N$. Moreover, the proposed image pixel reformations depend on qubit key matrix in which the pixel positions in the quantum plain image is reformed by referring to the positions (i, j) in the key matrix. In other words, adaptive quantum key matrix $|K\rangle$ produces different permutation matrix at each stage of the pixel reformation process and dynamic controlled image $|I_c\rangle$ is utilized for diffusion. Thus, different input image will have different key image and cipher image.

In general, an attacker in a classical cryptosystem can eavesdrop on the communication medium for accessing the plain image secret keys without modifying it. This allows the attacker to perform decryption at any time. However, in the proposed quantum-based medical image encryption scheme, given the initial conditions, attacker cannot be able to derive the quantum key matrix $|K\rangle$ without knowing the quantum state information. The probability of the quantum state of any qubits is $1/2$ and the proposed system has a qubit key matrix of size $n \times n$ thus the probability bound for obtaining a single key matrix for encrypting a single plain image is $1/2^n$ which is computationally infeasible. Thus, the proposed system can resist the chosen/known plain text attack.

4.1.12. Differential cryptanalysis

In general, differential cryptanalysis is a chosen plaintext attack where the attacker utilizes the knowledge about high probabilities of occurrences of a particular plaintext–ciphertext difference value. Assume, one-round encryption with $I_1, I_2, I_3, \ldots, I_n$ as input images and $C_1, C_2, C_3, \ldots, C_n$ as corresponding cipher images obtained from proposed encryption operation say pixel reformations and diffusion with a secret key. The proposed encryption operations are composed of quantum block-based scrambling, qubit rotations, transformations and diffusion. The pixel reformations are defined as

$$S_i^1 = f_S(|K\rangle(|I_{Q1}\rangle)), QR_i^1 = f_{QR}(|K\rangle(|I_{Q1}\rangle)), T_i^1 = f_T(|K\rangle(|I_{Q1}\rangle)), \quad i = 1, 2, 3..n \tag{20}$$

where, quantum scrambling S^1 is a function for mapping qubit key values and quantum image i.e.,

$$f_S(I^1_{Qi(x,y)}) = S^1_i(x_1, y_1), i = 1, 2, 3..n \tag{21}$$

similarly, other function f_{QR} and f_T can be defined. Let us assume ΔI_i be the input image differences and δC_i be the cipher image differences. Differential cryptanalysis uses the high probability of ΔC_i that is influenced by ΔI_i. The mathematical evaluation of differential attack is performed by considering two input images I_1, I_2 which is converted into quantum representation $|I_{Q1}\rangle$ and $|I_{Q2}\rangle$ and in turn the respective cipher images $|I_{Enc1}\rangle$ and $|I_{Enc2}\rangle$ are obtained by (22).

$$|I_{Enc}\rangle = |I_{Qst}\rangle Cnot |I_c\rangle \tag{22}$$

where, $|I_{Qst}\rangle$ is the permuted image, $|I_c\rangle$ is the key image obtained during the diffusion process. Generally, in classical cryptosystem, exclusive-or operation (XOR) is used as a substitution function and difference computation. However, in the proposed quantum-based image encryption, the controlled XOR is realized using CNOT quantum gates. The difference between $|I_{Enc1}\rangle$ and $|I_{Enc2}\rangle$ is represented as

$$\Delta Ci = |I_{Enc1}\rangle Cnot |I_{Enc2}\rangle \tag{23}$$

this can be rewritten as

$$\Delta C_i = (|I_{Qst1}\rangle Cnot |I_{c1}\rangle) Cnot (|I_{Qst2}\rangle Cnot |I_{c2}) \tag{24}$$

By expanding ΔC_i in terms of the quantum input image and qubit key matrix $|K\rangle$ and key image $|I_c\rangle$ (24) will become

$$\Delta C_i = ((|I_{Q1}\rangle Cnot |K_1\rangle) Cnot |I_{c1}\rangle) Cnot ((|I_{Q2}\rangle Cnot |K_2\rangle) Cnot |I_{c2}\rangle)$$

$$\Delta C_i = ((|I_{Q1}\rangle Cnot |I_{Q2}\rangle) Cnot (|K_1\rangle Cnot |K_2\rangle) Cnot (|I_{c1}\rangle Cnot |I_{c2}\rangle)) \tag{25}$$

From (25), it is clearly shown that, differential cipher image ΔC_i depends on $|K\rangle$ and $|I_c\rangle$. From these investigations, consider a scenario that, the attacker access the encryption machinery and choose sample blank images as one of the inputs and compute differential cipher images as given in (26). Also, if key values used in encryption scheme is independent of plain image and fixed then there exists same key values for different cipher image i.e., if $|K_1\rangle = |K\rangle$ and $|I_{c1}\rangle = |I_{c2}\rangle$ then attacker can easily access the plain image as

$$\Delta C_i = ((|I_{Q1}\rangle) Cnot (|K\rangle Cnot |K\rangle) Cnot (|I_c\rangle Cnot |I_c\rangle)) \tag{26}$$

$$\Delta C_i = (|I_{Q1}\rangle) \tag{27}$$

However, the proposed system utilizes plain image related key matrix and diffusion key image which generates different keys for different cipher image i.e., $|K_1\rangle \neq |K\rangle$ and $|I_{c1}\rangle \neq |I_{c2}\rangle$ Hence, Eq. (25) becomes,

$$\Delta C_i = |I_Q\rangle cnot |K_1\rangle Cnot |K_2\rangle Cnot |I_{c1}\rangle Cnot |I_{c2}\rangle \tag{28}$$

This shows that even after substituting the blank images during differential computation, the attacker will get two different keys during each stage of encryption. This results in high correlation among plain image, secret key and substitution key and guarantees the efficacy of the proposed cryptosystem towards differential cryptanalysis.

4.2. Perceptible quality of watermarked image

For guaranteeing the integrity of medical image, the ciphered regional data is embedded into encrypted cover medical image. Hence it is necessary to evaluate the proposed system with respect to visual quality of the watermarked image by using Peak Signal to Noise Ratio (PSNR) and Structural Similarity Measure Index (SSMI). The mathematical equation for PSNR and SSMI are expressed in (29) & (31). Table 13 shows the performance analysis of watermarked image.

Table 13
Perceptible analysis of watermarked images.

S.No	Encrypted image	PSNR	SSIM
1	Head CT	51.98	0.9713
2	Left arm X-ray	51.77	0.9856
3	Chest	51.38	0.9829
4	Spine MRI	51.28	0.9867
5	Brain MRI tumor	50.99	0.9929
6	CT scan breast cancer	51.29	0.9901
7	Mammography 1	51.43	0.9879
8	Abdomen CT	51.87	0.9932
9	Head CT 2	50.87	0.9853
10	Brain MRI 2	51.34	0.9967
11	Spine MRI - axial	51.43	0.9901
12	Left arm X-ray	50.98	0.9877
13	X-ray 2	49.98	0.9826
14	Coronary calcium scan 1	51.39	0.9845
15	Coronary calcium scan 2	51.41	0.9802
Average		**51.2967**	**0.9865**

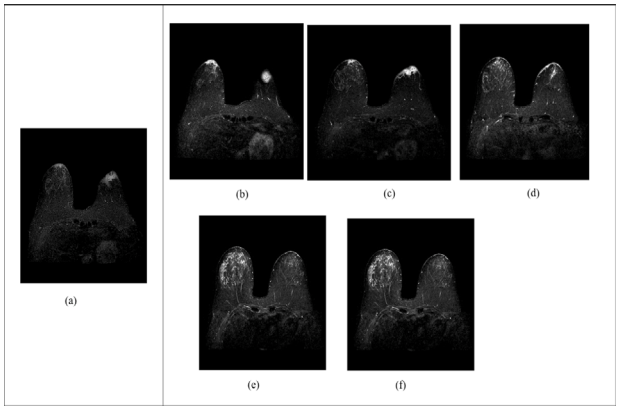

Fig. 19. (a) Query image of breast CT, (b)–(f) top query result of breast CT.

$$PSNR = 10 \log \frac{(255)^2}{MSE} db \tag{29}$$

where, MSE is Mean Square Error and it is defined as

$$MSE = \frac{1}{LK} \sum_{(i=1)}^{L} \sum_{(i=1)}^{K} (E_{ij} - E'_{ij})^2 \tag{30}$$

where L, K are the dimension of original and watermarked image and E_{ij} and E'_{ij} is the pixel value i, j in original and watermarked image respectively. Similarly, SSMI is defined as

$$SSIM = \frac{(2\varphi_{lk} + s_1)(2\sigma_{lk} + s_2)}{(\varphi_l^2 + \varphi_k^2 + s_1)(\sigma_l^2 + \sigma_l^2 + s_2)} \tag{31}$$

where φ is the mean, σ is the variance of L, K image pixels. The tabulated PSNR and SSIM estimation of test images shows the viability of proposed framework with respect to embedded image quality assessment.

4.3. Retrieval efficiency

The proposed system incorporates efficient identical image retrieval module by comparing the hashed image features with the help of suggested Interplanetary Image Features File System. The proposed framework also guarantees the privacy of medical image features by storing it as hashed values which are utilized for later images retrieval process. Fig. 19 depicts the query image and its retrieval results. Fig. 19

Table 14
Correlation and entropy estimations of proposed and existing approaches.

Scheme	Approach	Correlation			Entropy
		Horizontal	Vertical	Diagonal	
Ref. [3]		0.5310	–	–	7.95667
Ref. [6]		0.0965	−0.0318	0.0362	7.9852
Ref. [7]		−0.0147	0.0034	0.0619	7.9905
Ref. [8]		−0.0049	0.0030	−0.0052	7.9965
Ref. [9]		0.9911	−0.0080	0.0083	7.9995
Ref. [12]	Classical	−0.0015	−0.0032	−0.008	7.9972
Ref. [15]	cryptography	−0.0574	−0.0035	0.0578	7.9791
Ref. [16]		0.021	0.0004	−0.0038	7.9874
Ref. [17]		0.0056	−0.0876	–	–
Ref. [18]		0.0020	−0.0007	−0.0014	7.9972
Ref. [19]		0.001906418	0.0038175986	−0.0019482802	7.99705
Ref. [26]		0.00252	0.04741	–	7.9521
Ref. [31]		0.0018	0.0040	$-6.0096e^{-04}$	7.976
Ref. [33]		0.0213	0.0240	0.0143	7.786
Ref. [34]		0.00045	0.002175	0.003801	7.997
Ref. [35]	Quantum	−0.0026	−0.1457	−0.0069	7.884
Ref. [37]	cryptography	0.01918	0.01367	0.0158	7.9545
Ref. [39]		−0.00027	−0.0005	−0.0003	7.997
Ref. [40]		−0.00067	−0.000208	0.000268	7.996
Proposed scheme		**−0.00446**	**0.00103**	**0.00106**	**7.9993**

Table 15
Proposed diffusion mechanism vs. existing scheme.

Scheme	Parameters			
	PRNG (non-linear dynamics)	Quantum based diffusion	Plain image based keys	Adaptive diffusion
Ref. [3]	×	×	×	×
Ref. [11]	×	×	×	×
Ref. [26]	×	×	×	✓
Ref. [31]	✓	✓	×	×
Ref. [33]	×	✓	×	×
Ref. [35]	×	✓	×	×
Ref. [38]	✓	✓	×	×
Proposed system	✓	✓	✓	✓

Table 16
NPCR and UACI comparisons.

Ref.	Approach	NPCR	UACI
Ref. [3]	Mathematical based S-box	99.6287	31.8345
Ref. [6]	Chaos based one time key	99.66	33.4289
Ref. [7]	One-time key	99.6013	33.4210
Ref. [8]	One-time key	99.6032	33.52
Ref. [9]	Multimode image ciphering	99.96	33.39
Ref. [11]	Logistic-Chebyshev	99.61	28.42
Ref. [12]	Bit-level permutation	99.612	33.46
Ref. [15]	Bit-level permutation	99.6231	33.4959
Ref. [16]	DNA sequence	99.60	28.1370
Ref. [17]	Chaos and Perceptron network	76	–
Ref. [18]	DNA sequence operations &CML map	99.65	33.48
Ref. [19]	DNA & secure Arnold map	99.5864	33.253
Ref. [26]	Chaotic neural network	99.985	17.58
Ref. [31]	Quantum hyper chaos	99.6086	33.45
Ref. [33]	Qubit rotation	–	–
Ref. [34]	Quantum chaotic S-box	99.6119	33.40
Ref. [35]	Restricted geometric and color transformations	–	–
Ref. [37]	Selective encryption	–	–
Ref. [38]	Quantum walk	99.61204	–
Ref. [39]	Cascaded quantum walks with chaos inducement	99.60	–
Ref. [40]	One particle quantum walk	99.58	30.584
Proposed scheme	**Quantum block spatial transformations**	**99.7172**	**33.457**

clearly manifests that the proposed feature-based retrieval process results top five similar images efficiently with the help of image feature bucket table under encrypted scenario.

Table 17
Comparison of PSNR among proposed and various existing schemes.

Ref.	Security (approach)	PSNR	SSMI
Ref. [1]		27.5395	0.00616
Ref. [5]		38.10	0.4893
Ref. [23]	Classical cryptography	53.94	0.567
Ref. [20]		46.368	0.9827
Ref. [31]		8.5387	–
Ref. [45]	Quantum cryptography	48.041	–
Proposed scheme		**51.2967**	**0.9865**

Table 18
Computational time of proposed vs. existing approach for image 512 × 512.

Ref.	Approach	Encryption time (s)	Decryption time (s)
Ref. [3]		2.9766	3.152
Ref. [9]	Classical cryptography	1.028	1.002
Ref. [26]		21.04	25.7
Ref. [31]		3.546	2.987
Ref. [33]		2.12	2.19
Ref. [34]	Quantum cryptography	1.6772	1.546
Ref [43]		0.0069	–
Proposed scheme		**1.76**	**1.54**

5. Comparisons with existing approaches

The exploratory results of the suggested quantum encryption using spatial transformations is assessed with the conventional image encryption techniques e.g., mathematical based S-box [3], encryption based on one-time key [6–8], bit level permutation [12,15], DNA based model [16,18,19], chaotic-neural network encryption [17,26],medical ciphering [9] and quantum encryption methods [31,33–35,37–40,43,45] respectively. The advantages of the proposed scheme over the conventional method are, the suggested Quantum block based medical encryption method withstands the quantum cryptanalytic attacks as it utilizes quantum basic gates for generating keys and performing encryption function. To attain high sensitivity with respect to plain image, the suggested scheme uses plain image related initial keys and diffusion process. As a result, this shows a very good range of Number of Pixel change rate and UACI values. Similarly, it exhibits the key value of 10^{180} which makes brute force attack to be ineffective.

Table 19
Qualitative feature comparisons for medical image integrity.

Features	Ref. [24]	Ref. [20]	Ref. [22]	Ref. [45]	Ref. [37]	Proposed scheme
Plain image based key	×	×	×	×	×	✓
Image encryption	✓	✓	✓	✓	Selective	✓
ROI encryption	×	×	×	×	✓	✓
one-time pad (ROI)	×	×	×	×	×	✓
Security (quantum)	×	×	×	×	✓	✓
Tamper detection	×	✓	×	×	×	✓
Block size	4 × 4	4 × 4	Key based	–	–	3 × 3
Recovery procedure	×	✓	×	×	×	✓
Perception quality	✓	✓	✓	✓	×	✓

5.1. Quantitative measures for validating image confidentiality

Table 14 shows the comparison and effectiveness of the proposed quantum cryptosystem system towards the randomness and hiding of adjacent pixel correlation. Yet, Refs. [39,40] have less correlation as they include quantum-inspired random walks for pixel scrambling and diffusion, but it has less NPCR and UACI values.

The security of any image encryption scheme profoundly relies upon the diffusion process as it changes the pixel values in addition to relocating it. The proposed diffusion phase utilizes Arnold cat map for producing NEQR key image $|I_c\rangle$ later the Controlled NOT gate is applied over the scrambled image I_Q^{st} and $|I_c\rangle$. The randomness of the cipher image depends on the NEQR key image. Table 15 shows the comparisons of parameter adopted in proposed diffusion method with state-of -art method. Also, the strength of the diffusion process can be examined by analyzing the number of pixel change rate once it is XOR-ed with the key image. From Table 16, it is evident that the proposed scheme exhibits NPCR value as 99.78% which shows the higher diffusion performance and the proposed scheme outperforms well among the notable existing schemes including [11,38–40].

5.2. Quality of encrypted and watermarked images

The proposed framework ensures two levels of security for the medical image by incorporating quantum block-based image encryption and ROI regional data encryption. The performance comparison of ROI region data encryption embedded on watermarked image with various schemes are shown in Table 17.

5.3. Time analysis

The execution speed is a significant standard for evaluating encryption algorithms [43]. The execution time for encrypting the medical images with varying dimensions are listed out in Table 18. The comparative study is carried out for understanding the efficiency of the proposed algorithm among different conventional schemes and the outcomes are figured out in Table 18 which shows that the proposed system has better computational time than other available schemes.

5.4. Qualitative analysis for validating image integrity

The Qualitative analysis of the proposed scheme is performed by comparing various features like encryption, block size, tamper detection for preserving image integrity, security metrics, recovery metrics, resistance against differential attack, perception quality of watermarked image of the proposed system with respect to different conventional schemes and listed in Table 19. The proposed scheme utilized plain image based initial seed generation phase for encrypting the medical image which increases the key and image sensitivity towards intruders. Additionally, it encrypts both the image and sensitive region of the image separately which provides the complete shield for medical image along ROI data while outsourcing it. Also, the proposed system consists of dedicated modules as tamper detection for ensuring the image trustworthiness. The proposed system possess very good perceptible quality of regional data embedded images. Thus, from the above discussions, it is indicated that the proposed image and ROI encryption outperform the notable existing approaches and it maintains the secrecy and trustworthiness of the medical images over the outsourced environment.

6. Conclusion

A new quantum-based medical image encryption scheme has been proposed with two levels of security: A novel quantum block-based image encryption using spatial transformation for preserving confidentiality and medical image ROI regional data encryption for ensuring trustworthiness. The interplanetary feature file system is suggested for the efficient retrieval of medical images in bilateral transmissions. The suggested qubit key matrix holds the uncertainty principles of quantum mechanics and produces different shuffled vectors for different image permutation and diffusion. The numerical simulations are carried out in MATLAB and it results in better uniformity, minimal correlation among encrypted pixels, and superior randomness rate in an encrypted image. With these experimental results, it is evident that the proposed system has high resistance towards statistical and differential attack. Additionally, as the medical images are encrypted using quantum cryptosystem, it is able to combat the quantum cryptanalytic attacks using quantum machines.

CRediT authorship contribution statement

T. Janani: Conceptualization, Methodology, Design of study, Software, Writing - original draft. **M. Brindha:** Supervision, Investigation, Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Laiphrakpam DS, Khumanthem MS. Medical image encryption based on improved elgamal encryption technique. Optik 2017;147:88–102.
[2] Kanso A, Ghebleh M. An efficient and robust image encryption scheme for medical applications. Commun Nonlinear Sci Numer Simul 2015;24(1–3):98–116.
[3] Çavuşoğlu Ü, Kaçar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based s-box. Chaos Solitons Fractals 2017;95:92–101.
[4] Artiles JA, Chaves DP, Pimentel C. Image encryption using block cipher and chaotic sequences. Signal Process, Image Commun 2019;79:24–31.
[5] Xingyuan W, Junjian Z, Guanghui C. An image encryption algorithm based on zigzag transform and LL compound chaotic system. Opt Laser Technol 2019;119:105581.
[6] Liu H, Wang X. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59(10):3320–7.
[7] Dong C. Color image encryption using one-time keys and coupled chaotic systems. Signal Process Image Commun 2014;29(5):628–40.
[8] Khedr WI. A new efficient and configurable image encryption structure for secure transmission. Multimedia Tools Appl 2019;1–25.

[9] Boussif M, Aloui N, Cherif A. Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition. IET Image Process 2017;11(11):1020–6.
[10] Hua Z, Yi S, Zhou Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Process 2018;144:134–44.
[11] Abd-El-Atty B, Amin M, Abd-El-Latif A, Ugail H, Mehmood I. An efficient cryptosystem based on the logistic-Chebyshev map. In: 2019 13th international conference on software, knowledge, information management and applications (SKIMA). IEEE; 2019, p. 1–6.
[12] Li Y, Wang C, Chen H. A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Opt Lasers Eng 2017;90:238–46.
[13] Chen X, Hu C-J. Adaptive medical image encryption algorithm based on multiple chaotic mapping. Saudi J Biol Sci 2017;24(8):1821–7.
[14] Boriga R, Dăscălescu AC, Priescu I. A new hyperchaotic map and its application in an image encryption scheme. Signal Process, Image Commun 2014;29(8):887–901.
[15] Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284(16–17):3895–903.
[16] Liu H, Wang X, et al. Image encryption using dna complementary rule and chaotic maps. Appl Soft Comput 2012;12(5):1457–66.
[17] Wang X-Y, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynam 2010;62(3):615–21.
[18] Wang X-Y, Zhang Y-Q, Bao X-M. A novel chaotic image encryption scheme using dna sequence operations. Opt Lasers Eng 2015;73:53–61.
[19] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;66:10–8.
[20] Parah SA, Ahad F, Sheikh JA, Bhat GM. Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform 2017;66:214–30.
[21] Das S, Kundu MK. Effective management of medical information through roi-lossless fragile image watermarking technique. Comput Methods Programs Biomed 2013;111(3):662–75.
[22] Murali P, Sankaradass V. An efficient roi based copyright protection scheme for digital images with svd and orthogonal polynomials transformation. Optik 2018;170:242–64.
[23] Bouslimi D, Coatrieux G, Cozic M, Roux C. A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inf Technol Biomed 2012;16(5):891–9.
[24] Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A. Secure medical data transmission model for iot-based healthcare systems. Ieee Access 2018;6:20596–608.
[25] Wang X, Feng L, Zhao H. Fast image encryption algorithm based on parallel computing system. Inform Sci 2019;486:340–58.
[26] Dridi M, Hajjaji MA, Bouallegue B, Mtibaa A. Cryptography of medical images based on a combination between chaotic and neural network. IET Image Process 2016;10(11):830–9.
[27] Wang X, Gao S. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. Inform Sci 2020;507:16–36.
[28] Wang X, Gao S. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a boolean network. Inf Sci 2020;539:195–214.
[29] Cho K, Miyano T. Chaotic cryptography using augmented lorenz equations aided by quantum key distribution. IEEE Trans Circuits Syst I Regul Pap 2014;62(2):478–87.
[30] Akhshani A, Akhavan A, Lim S-C, Hassan Z. An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 2012;17(12):4653–61.
[31] Luo Y, Tang S, Liu J, Cao L, Qiu S. Image encryption scheme by combining the hyper-chaotic system with quantum coding. Opt Lasers Eng 2020;124:105836.
[32] Yan F, Iliyasu AM, Le PQ. Quantum image processing: a review of advances in its security technologies. Int J Quantum Inf 2017;15(03):1730001.
[33] Liu X, Xiao H, Li P, Zhao Y. Design and implementation of color image encryption based on qubit rotation about axis. Chin J Electron 2018;27(4):799–807.
[34] Liu H, Zhao B, Huang L. Quantum image encryption scheme using arnold transform and s-box scrambling. Entropy 2019;21(4):343.
[35] Song X-H, Wang S, Abd El-Latif AA, Niu X-M. Quantum image encryption based on restricted geometric and color transformations. Quantum Inf Process 2014;13(8):1765–87.
[36] Liu X, Xiao D, Xiang Y. Quantum image encryption using intra and inter bit permutation based on logistic map. IEEE Access 2018;7:6937–46.
[37] Heidari S, Naseri M, Nagata K. Quantum selective encryption for medical images. Internat J Theoret Phys 2019;58(11):3908–26.
[38] Abd El-Latif AA, Abd-El-Atty B, Venegas-Andraca SE, Elwahsh H, Piran MJ, Bashir AK, Song O-Y, Mazurczyk W. Providing end-to-end security using quantum walks in iot networks. IEEE Access 2020.
[39] Abd el Latif AA, Abd-el Atty B, Amin M, Iliyasu AM. Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci Rep 2020;10(1):1–16.
[40] Abd-El-Atty B, Abd El-Latif AA, Venegas-Andraca SE. An encryption protocol for neqr images based on one-particle quantum walks on a circle. Quantum Inf Process 2019;18(9):272.
[41] Abd EL-Latif AA, Abd-El-Atty B, Abou-Nassar EM, Venegas-Andraca SE. Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. Opt Laser Technol 2020;124:105942.
[42] Abd EL-Latif AA, Abd-El-Atty B, Venegas-Andraca SE. Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption. Physica A 2019;123869.
[43] Abd El-Latif AA, Abd-El-Atty B, Mazurczyk W, Fung C, Venegas-Andraca SE. Secure data encryption based on quantum walks for 5g internet of things scenario. IEEE Trans Netw Serv Manag 2020;17(1):118–31.
[44] Song X-H, Wang H-Q, Venegas-Andraca SE, Abd El-Latif AA. Quantum video encryption based on qubit-planes controlled-xor operations and improved logistic map. Physica A 2020;537:122660.
[45] Abd El-Latif AA, Abd-El-Atty B, Hossain MS, Rahman MA, Alamri A, Gupta BB. Efficient quantum information hiding for remote medical image sharing. IEEE Access 2018;6:21075–83.
[46] Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceeding 2000 IEEE symposium on security and privacy. S&P 2000. IEEE; 2000, p. 44–55.
[47] Chang Y-C, Mitzenmacher M. Privacy preserving keyword searches on remote encrypted data. In: International conference on applied cryptography and network security. Springer; 2005, p. 442–55.
[48] Zhang Y-Q, Wang X-Y. A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 2015;26:10–20.
[49] Wu Y, Noonan JP, Agaian S, et al. Npcr and uaci randomness tests for image encryption. Cyber J Multidiscip J Sci Technol J Sel Areas Telecommun (JSAT) 2011;1(2):31–8.
[50] Zhang Y-Q, Wang X-Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inform Sci 2014;273:329–51.
[51] Li C, Zhang Y, Xie EY. When an attacker meets a cipher-image in 2018: A year in review. J Inf Secur Appl 2019;48:102361.
[52] Ma Y, Li C, Ou B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. J Inf Secur Appl 2020;54:102566.
[53] Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Process 2012;92(4):1101–8.
[54] Benrhouma O, Hermassi H, Abd El-Latif AA, Belghith S. Cryptanalysis of a video encryption method based on mixing and permutation operations in the dct domain. Signal Image Video Process 2015;9(6):1281–6.
[55] Bechikh R, Hermassi H, Abd El-Latif AA, Rhouma R, Belghith S. Breaking an image encryption scheme based on a spatiotemporal chaotic system. Signal Process, Image Commun 2015;39:151–8.