Contents lists available at ScienceDirect

Internet of Things

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

Research article

Securing Medical Information Transmission Between IoT Devices: An Innovative Hybrid Encryption Scheme Based on Quantum Walk, DNA Encoding, and Chaos

Mujeeb Ur Rehman [a,*], Arslan Shafique [a], Aminu Bello Usman [b]

[a] School of Science, Technology and Health, York St John University, York, UK
[b] School of Computer Science, University of Sunderland, UK

ARTICLE INFO

Keywords:
Medical image encryption
Quantum cryptography
DNA encoding
Color image encryption
Multilayered encryption

ABSTRACT

The healthcare industry has undergone a transformation due to the widespread use of advanced communication technologies and wireless sensor networks such as the Internet of Medical Things (IoMT), Health Information Exchange Technology (HIET), Internet of Healthcare Things (IoHT) and Health IoT (HIoT). These technologies have led to an increase in the transmission of medical data, particularly medical imaging data, over various wireless communication channels. However, transmitting high-quality color medical images over insecure internet channels like the Internet and communication networks like 5G presents significant security risks that could threaten patients' data privacy. Furthermore, this process can also burden the limited bandwidth of the communication channel, leading to delayed data transmission. To address security concerns in healthcare data, researchers have focused a lot of attention on medical image encryption as a means of protecting patient data. This paper presents a color image encryption scheme that integrates multiple encryption techniques, including alternate quantum random walks, controlled Rubik's Cube transformations, and the integration of the Elliptic Curve Cryptosystem with Hill Cipher (ECCHC). The proposed scheme divides various plaintext images by creating a regular cube by layering planes of a fixed size. Each plane is rotated in an anticlockwise direction, followed by row, column and face swapping, and then DNA encoding is performed. The image cube encoded with DNA is combined with the chaotic cube through DNA addition, and a couple of random DNA sequences are chosen for DNA mutation. After undergoing DNA mutation, the encoded cube is then decoded using DNA. The proposed method has the theoretical capability of encrypting 2D images of unlimited size and number by utilizing an infinitely large cube. The proposed image encryption scheme has been rigorously tested through various experimental simulations and cyberattack analysis, which shows the efficiency and reliability of the proposed encryption scheme.

1. Introduction

Telemedicine, a rapidly growing field enabled by the Internet of Things (IoT), revolutionizes healthcare delivery by facilitating remote medical care. Through interconnected devices and sensors, IoT technologies enable the uninterrupted transmission of medical images, patient data, and other critical information over the internet or cellular networks. This interconnected system provides healthcare providers with real-time access to patient data regardless of their physical location, fostering timely and

[*] Corresponding author.
E-mail addresses: m.rehman@yorksj.ac.uk (M.U. Rehman), arslanshafique762@gmail.com (A. Shafique), aminu.usman@sunderland.ac.uk (A.B. Usman).

https://doi.org/10.1016/j.iot.2023.100891
Received 2 June 2023; Received in revised form 10 July 2023; Accepted 1 August 2023
Available online 25 August 2023

informed decision-making. Furthermore, IoT devices play a pivotal role in monitoring patients' health remotely, collecting vital signs, and transmitting data to healthcare professionals, enabling proactive interventions and reducing the need for hospital visits. However, the widespread adoption of IoT in telemedicine also raises concerns about data privacy and security. Safeguarding sensitive patient information and ensuring secure communication channels become imperative in the IoT-enabled telemedicine landscape. Robust encryption algorithms, secure data storage systems, and stringent access control mechanisms are vital to protecting patient privacy and mitigating the risks associated with cyber threats. As the IoT continues to advance, it holds great potential in transforming healthcare delivery by enabling remote patient monitoring, facilitating teleconsultations, and enhancing overall healthcare accessibility and efficiency. With the continuous advancement in information transmission between IoT devices, ensuring the robust security of sensitive medical information contained within medical images against cyberattacks has become a challenging task. To address this issue, numerous encryption schemes have been introduced to protect medical images by rendering them useless to unauthorized users without encryption information. Various security solutions for telemedicine applications are explored and discussed in [1]. Preserving the security and confidentiality of data is necessary, especially concerning medical images, which serve as essential information carriers across multiple sectors, including healthcare. Unfortunately, medical images are prone to interception and tampering during transmission, which poses a significant threat to the privacy of patients' data [2]. To address the security concerns of medical images, numerous researchers have proposed various image encryption techniques. For instance, some digital image encryption methods utilize chaotic systems [3], which generate random sequences to control the pixel's position. Others rely on encryption techniques such as the discrete cosine transform, discrete wavelet transform, and Fourier transform [4] noise that converts image pixels into the frequency domain. Other classical encryption techniques include frequency transformation encryption, DNA-based encoding encryption and chaotic encryption [5]. The chaos theory gained significant attention due to its numerous robust cryptographic properties, such as its large key space and sensitivity to initial conditions. As a result, this theory could provide various benefits for the encryption of medical images. Therefore, researchers in the field of medical image security and secure communication have focused on developing single-image encryption (SIE) and multiple-image encryption (MIE) schemes that utilize chaotic systems, making it a popular area of research.

In addition to chaos-based medical encryption, Rubiks' cube (RC)based image encryption algorithms have also been proposed in recent years [6]. The RC transformation operates by altering the positions of sub-blocks in order to scramble the cube. Similarly, applying this transformation to images involves rearranging the positions of individual pixels to achieve a scrambled output. With a third-order RC, rotating a single layer by 90 degrees can result in eighteen distinct rotational configurations. Although there are many ways to permute and combine a 3rd-order RC, there is only one way to restore it, which results in high computational complexity. As a result, merging the transformation of RC with image encryption is a feasible alternative. Zhang et al. [7] utilized a combination of chaotic sequences and RC transformations to introduce a new image encryption scheme to secure the grayscale images. On the other hand, Loukhaoukha et al. [8] provide the solution to secure digital images that leverages the rotational principle of the RC. This encryption algorithm effectively scrambles and encrypts images using RC rotation, but its key space is limited. Vidhya et al. [9] proposed an image encryption algorithm based on a chaotic map that utilizes RC transformation. This proposed method fully utilizes the principles of RC to achieve bit-level image encryption and a strong scrambling effect.

Apart from encryption schemes based on RC, various researchers have proposed the use of Hill cipher encryption as a means of providing a suitable level of security for digital images. For instance, [10] developed HillMRIV, a novel Hill cipher that uses a unique secret key for each plaintext block rather than employing a single secret key for all blocks. Although this approach improves the security of the Hill algorithm, its effectiveness is restricted by the presence of plaintext blocks consisting only of zeros. In contrast, Acharya et al. [11] addressed the challenge of the inversion of the key matrix not being present by devising an innovative advanced Hill algorithm known as AdvHill. By employing a shared key matrix for encrypting and decrypting the plaintext images, there is no longer a need for the recipient to compute the inverse key matrix. Additionally, it enhances cipher randomization, leading to improved algorithm efficiency. Hamissa et al. [12] enhanced the security of the Hill cipher algorithm by integrating a logistic map and introducing a novel encoder–decoder technique to secure digital images. Similarly, a three-step strategy was proposed by Panduranga et al. [13] to enhance the entropy of the encrypted image using the Hill cipher. Rahman et al. [14] introduced Hill++, a novel Hill algorithm that produces an extra key for encryption by generating a random key matrix and is capable of processing plaintext blocks that comprise only of zeros. This algorithm integrates the Hill cipher with the affine cipher to enhance its resistance against cyberattacks. Agrawal et al. [15] proposed a Hill cipher-based innovative encryption technology to create ciphertext values that are subsequently transformed into points on the ECC.

Recently, significant progress and development have been made in MIE algorithms that are based on chaotic systems. For instance, Tang et al. [16] proposed a method that involves bit-plane extraction and chaotic maps to produce noisy images. Hua et al. [17] developed an MIE algorithm that encrypts multiple plaintext images into a single encrypted image using the SIE method. Li et al. [18] combined a compression scheme in their MIE algorithm to enhance the security of the encrypted images while reducing storage space. Rasul et al. [19] proposed a new approach where all the images are merged into a single large image, and subsequently, they are organized as one-dimensional data for the encryption process. Gao et al. [20] developed an MIE scheme that encrypts multiple images using optical methods, which can be expensive and have practical limitations, while Sahasrabuddhe et al. [21] employed a technique that breaks multiple color images into small blocks and stacks them into cubes for encryption. Although these schemes demonstrate effectiveness, certain algorithms have limited key spaces, making them susceptible to brute-force attacks. Others rely on expensive optical methods, and some fail to conceal the statistical properties of the image sufficiently, leading to security performance shortcomings.

In this research, a new color image encryption algorithm for medical images is proposed that utilizes a 3D cube and hyperchaotic map. This algorithm effectively overcomes the limitation of the number of encrypted images that can be processed. Moreover, the proposed encryption scheme incorporates alternative quantum random walks, DNA operations, and chaos. The quantum walk is applied to alter the original pixel values through the walk operator, which facilitates the transition of the quantum state across a graph structure. Subsequently, the modified pixel values undergo further transformations using DNA operations, where each altered pixel value is associated with a specific DNA sequence or combination of nucleotides. After that, chaos is employed by utilizing a hyper-chaotic map to generate key sequences. This inclusion of chaos enhances resistance against brute force attacks by generating a significantly larger keyspace.

Finally, the proposed encryption approach employs ECC for generating private keys, enabling both the sender and receiver to generate the secret key without sharing it over the internet or an insecure communication channel. However, the Hill cipher algorithm has a significant limitation in that the inverse of the key matrix may not always exist. If the key is non-reversible, decrypting the data becomes impossible, leaving the recipient unable to access the plaintext. However, this problem is resolved in this research by utilizing a reversible key matrix, where the key can be reversed. Moreover, this technique also reduces the computational complexity required for computing the key matrix inverse during the encryption process. Further, the proposed encryption scheme offers several advantages, such as a large key space, high sensitivity to secret keys, low key management overhead (LKMO), and resistance to cyberattacks, including brute force attacks, and chosen or known plaintext attacks.

To develop a proposed encryption scheme, the contributions to the paper are as follows:

1. A new encryption scheme to secure color medical images that incorporates a 3D cube and hyperchaotic is proposed.
2. The proposed encryption scheme combines various encryption techniques, including alternate quantum walk, controlled RC transformation, and the integration of the ECC with Hill Cipher. This combination of encryption techniques results in a highly efficient encryption scheme in terms of high security and low computational complexity.
3. The key generation process involves ECC which ensures that the sender and receiver can generate the secret keys without sharing them over an insecure channel such as the internet end. This also enhances the robustness of the secure keys and thereby increasing the robustness of the proposed encryption scheme.
4. The self-reversible key matrix helps to reduce the computational overhead during the decryption process.
5. Various experimental results and analysis such are information entropy, histogram variance, correlation, energy, entropy analysis, etc. are conducted to gauge the effectiveness of the proposed encryption scheme. Moreover, in order to show the resilience of the proposed encryption scheme against a range of cyberattacks, including cropping attacks, brute force attacks, noise attacks, and lossless attacks, multiple attack simulations are conducted.

2. Quantum walks

The proposed research focuses on the discrete-time quantum random walk (DWQW). The DWQW primarily consists of two main components, namely the coin space ($\mathcal{H}^C$) and rambler's space ($\mathcal{H}^L$). As a result, the quantum walk may be represented within the Hilbert space denoted as $\mathcal{H} = \mathcal{H}^C \bigotimes \mathcal{H}^L$, where $\mathcal{H}^C$ represents the two-dimensional Hilbert space of the coin state [22]. The quantum random walk consists of two main stages in its process. In the first stage, the coin operator is applied to the coin state within $\mathcal{H}^C$. The second stage involves the application of the unitary operator ($\hat{\bigcup}$) to the complete $\mathcal{H}$. Therefore, the quantum walk can be perceived as the iterative application of the unitary operator on the quantum walk system. Mathematically, the operator $\hat{\bigcup}$ can be expressed as given in Eq. (1).

$$\hat{\bigcup} = \mathbf{T}O = \mathbf{T}(\hat{O} \bigotimes I) \tag{1}$$

Let the quantum walk coin operator consistently select the operator $\hat{O}$:

$$\hat{O} = \begin{bmatrix} cos\beta & sin\beta \\ -\sin\beta & cos\beta \end{bmatrix} \tag{2}$$

When the angle $\beta = \frac{\pi}{4}$, the coin operator can be represented as follows:

$$\hat{O} = \frac{1}{\sqrt{2}} \begin{bmatrix} cos(\frac{\pi}{4}) & sin(\frac{\pi}{4}) \\ -sin(\frac{\pi}{4}) & cos(\frac{\pi}{4}) \end{bmatrix} = H$$

$$\hat{O} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = H \tag{3}$$

Quantum walks employ the transfer operator **T** to influence the walker's directional choice for the next step. If the coin state is in the $|0\langle$ (spin up ↑) condition, the walker will proceed in a particular direction. On the other hand, if the coin state is in the $|1\langle$ (spin up ↓) condition, the walker will take a step in the reverse direction. Consequently, the transfer operator **T** can be expressed as follows:

$$\mathbf{T} = |0\rangle\langle 0| \otimes |m+1|1\rangle\langle 1 \otimes |m-1\rangle\langle m| \tag{4}$$

The alternate quantum walk operates in a two-dimensional space where the position state tensor $\{|\mathbf{A}, \mathbf{B}, a, b \in \mathbb{Z}\}$ enables the walker to alternate between two directions. As a result, the expression for the unitary operator, which iteratively operates on the quantum walk system during the process of quantum random walk, is mentioned in Eqs. (5), (6), and (7):

$$\hat{\bigcup} = \hat{\mathbf{T}}_b(I \otimes \hat{O})\hat{\mathbf{T}}_a(I \otimes \hat{O}) = \hat{\mathbf{T}}_b(I \otimes H)\hat{\mathbf{T}}_a(I \otimes H) \tag{5}$$

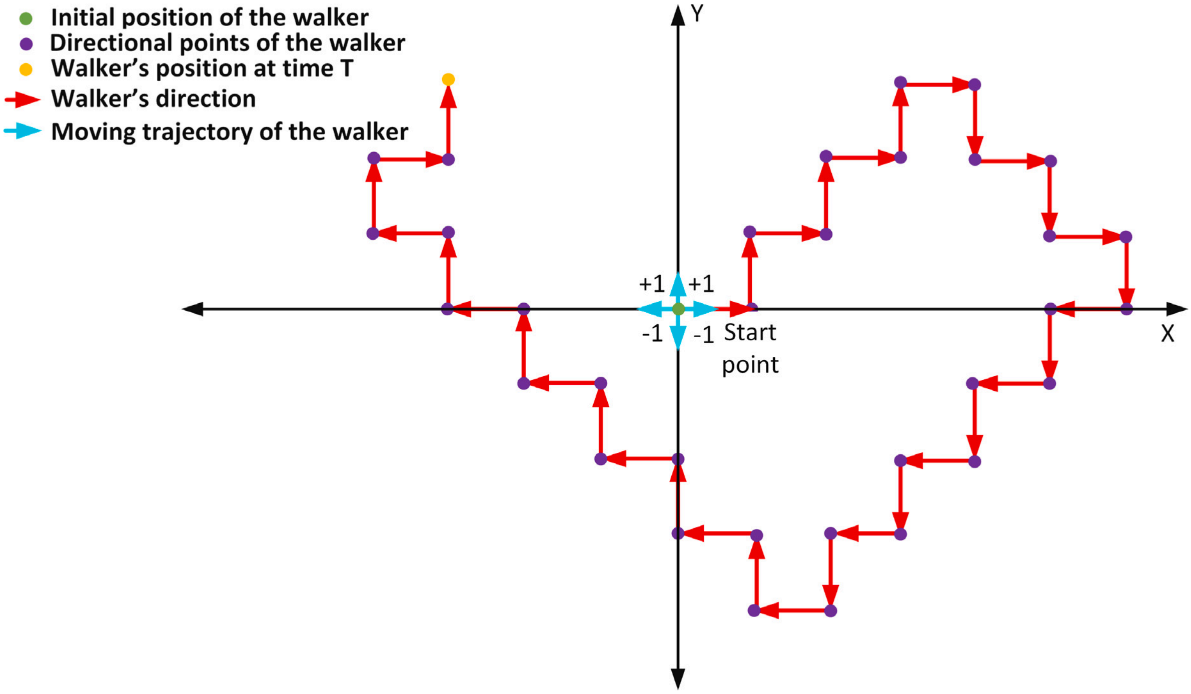

Initial position of the walker
Directional points of the walker
Walker's position at time T
Walker's direction
Moving trajectory of the walker
Y
X
+1
+1
-1
-1
Start point

Fig. 1. Quantum walk.

$$\hat{\mathbf{T}}_b = |0\rangle\langle 0| \otimes \sum_{n,m\in\mathbb{Z}} |m+1,n\rangle\langle m,n| + |1\rangle\langle 1| \otimes \sum_{n,m\in\mathbb{Z}} |m-1,n\rangle\langle m,n| \tag{6}$$

$$\hat{\mathbf{T}}_a = |0\rangle\langle 0| \otimes \sum_{n,m\in\mathbb{Z}} |m+1,n\rangle\langle m,n| + |1\rangle\langle 1| \otimes \sum_{n,m\in\mathbb{Z}} |m-1,n\rangle\langle m,n| \tag{7}$$

If the coin is in the state $|0\rangle(|1\rangle)$, the walker will be directed to move up (down) along the Y-axis and move right (left) along the X-axis, as illustrated in Fig. 1. At the starting moment, assuming the walker is initially at the local position $(x, y) = (0, 0)$, and the coin state is in a superposition state $|\text{coin}\rangle = x|0\rangle + y|1\rangle$, the quantum walk's starting state can be expressed as $|\nexists_0\rangle = |00\rangle \otimes |coin\rangle$. Upon completing N steps, the quantum state of the whole system is represented as $\nexists_M\rangle = \hat{\bigcup}^M |\nexists_0\rangle$, and the mathematical form for the probability of locating the walker at position (y, x) is provided in Eq. (8). Algorithm 1 outlines the procedure for employing quantum walk in the proposed encryption algorithm.

$$P_{X,Y} = \sum \left|\left\langle y,x,0\middle|\hat{\bigcup}^M\middle|\nexists_0\right\rangle\right|^2 + \sum \left|\left\langle y,x,1\middle|\hat{\bigcup}^M\middle|\nexists_0\right\rangle\right|^2 \tag{8}$$

3. Rubik's cube transform

The idea of RC transformation is derived from the RC toys, which involve manipulating the cube's surface patterns by rotating its segments.

The proposed encryption scheme is designed for a third-order RC, consisting of 26 sub-blocks, and is capable of rotation along any axis. The encryption technique proposed in this research is tailored to a RC of the third-order, comprising 26 sub-blocks, and is capable of being rotated in any orientation. The color of each face of the cube is different.

To solve a 3rd-order RC, the arrangement of the six faces and the identification of each sub-block must be established. The expansion map for a 3rd-order RC is shown in Fig. 2, with the top side referred to as A, the front side as B, the right side as C, the bottom side as D, the back side as E, and the left side as F. As the A and D surfaces, C and F surfaces, and B and E surfaces are interconnected, our focus is limited to three surfaces: A, C, and B. For example, if we turn the first layer of the A side by 90^0 to the right, the resulting state of the Cube is demonstrated in Fig. 2. The A surface rotates counterclockwise by 90^0, while the D surface remains unaltered. If we rotate the middle layer of the A side by 90^0, the middle layers of the B, C, E, and F sides are cyclically shifted, while the A and D surfaces remain the same. The same principle applies to the rotation of the other surfaces, employing a similar approach.

Algorithm 1 Pseudo code for generating random sequence using quantum walk in H^C and H^L space

```
Start

→ Initialize the number of states and steps;

NoOfSteps = 256;

NoOfStates = 2;

→ Define the initial state of the walker

psi_location = zeros(NoOfStates, 1);
→ Set the initial position

        psi_loc($\frac{NoOfStates+1}{2}$) = 1;
→ Define the coin operator/space $H^C$
→ Apply Hadmard coin as follows:
        $H = \frac{1}{\sqrt{2}} \times [11; 1-1];$
→ The Hadamard coin maps the basis states $\left|0\right\rangle$ and $\left|1\right\rangle$ to an equal superposition of the two states
        $H\left|0\right\rangle = \frac{1}{\sqrt{2}} \times (\left|0\right\rangle + \left|1\right\rangle)$
        $H\left|1\right\rangle = \frac{1}{\sqrt{2}} \times (\left|0\right\rangle - \left|1\right\rangle)$
coin = hadamard(2);
→ Defining the shift operator
        shift = circshift(eye(NoOfStates), [0, -1]) + circshift(eye(NoOfStates), [0, 1]);
        shift(1, NoOfStates) = 0;
        shift(NoOfStates, 1) = 0;
→ Develop the quantum walk operator in $H^C$ and $H^L$
        quantumWalk = kron(coin, eye(NoOfStates)) × kron(eye(2), shift);
→ Use the quantum walk operator to the initial state
        psi = $(quantumWalk)^{NoOfSteps} \times kron([1; 0], psi_loc);$
→ Locate the final state in the location space
        probDist = abs(psi(numStates+1:end))$^2$;
        plot(1:noOfStates, probDist);
        xlabel('Position');
        ylabel('Probability');
End
```

By utilizing the aforementioned principles, the *RC* rotations can be used to create a particular pattern or disrupt an existing one. This theory of *RC* transformations can be implemented in image encryption. In the proposed scheme, the image's pixels are mapped onto the *RC*, and each sub-block of the cube represents a pixel of the image. The original image's pixel positions are shuffled using a specific scrambling rule based on the principles of *RC* transformations, resulting in an irregular image. To decrypt the encrypted image and obtain the original image, the recipient must possess the appropriate key. Therefore, this technique enhances the confidentiality and security of image information during transmission.

4. Elliptic curve (EC) operations with Hill cipher (HC)

The primary operation in EC that requires the most time during encryption and decryption is scalar multiplication, which is reliant on both point addition and point doubling [23].

4.1. Point addition

Choose any two points such as $P_1 = (a_1, b_1)$ and $P_2 = (a_2, b_2)$ that must lie on the same curve. Adding P_1 and P_2 as shown in Eq. (9) will give the third point T that should also lie on the same curve.

$$T = P_1 + P_2 = (a_3, b_3) \tag{9}$$

Where,

$$\text{Slope } (R) = \frac{(b_2 - b_1)}{(a_2 - a_1)}$$

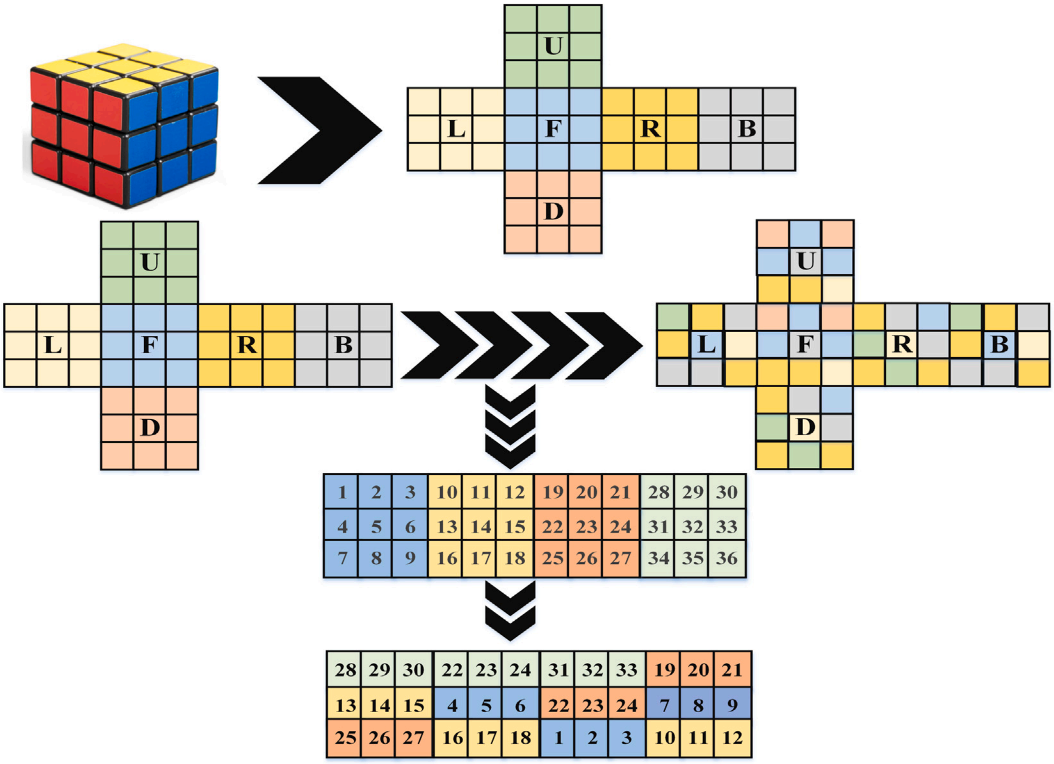


Fig. 2. Third order RC principle.

$$a_3 = (R^2 - a_1 - b_2)(mod\, P)$$

$$b_3 = (Ra_1 - Ra_3 - b_1)(mod\, P)$$

4.2. Point doubling

When a point $P = (a_1, b1)$ on the elliptic curve E is added to itself, it is referred to as "point doubling" as given in Eq. (10). The outcome of doubling point P is point T, which is also situated on the elliptic curve E.

$$T = 2P = P + P = (a_3, b_3) \tag{10}$$

Where,

$$R = \frac{3x_1^2 + c}{2b_1}$$

$$b_3 = (R^2 - 2a_1)(mod\, P)$$

$$b_3 = (Ra_1 - Ra_3 - b_1)(mod\, P)$$

4.3. Scalar multiplication

A point $M = (a_1, b1)$ located on the curve E can be multiplied by an integer Z via scalar multiplication, which involves adding point M to itself Z times. As a result, point T is generated, and it also belongs to the elliptic curve E as given in Eq. (11).

$$T = ZM = \underbrace{M + M + M + \cdots + M}_{\text{Z-times}} \tag{11}$$

An instance of this is calculating 15Q, which can be achieved through point addition and point doubling operations in the following manner as given in Eq. (12):

$$15M = 2(2(2M + M) + M) + M \tag{12}$$

Table 1
Rules for DNA encoding in the proposed encryption scheme.

00	A	G	C	T	G	C	A	T
01	C	A	G	G	T	C	A	T
10	C	T	G	C	T	A	A	G
11	T	T	A	C	A	G	C	G

Table 2
DNA encoding rule with XOR operation.

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

4.4. Hill cipher

The fundamental principle behind this technique involves the assignment of a numerical value to each letter [24], such as $a = 0, b = 1$, and so on, up to $z = 25$. Next, tThe original message is segmented into uniformly sized blocks k, which depends on the size of the key matrix $k \times k$. If the block size is, for example, two $(B_{2\times1})$, then the key matrix $(S_{2\times2})$ must be of the size 2×2. In the encryption process, the enciphered block, consisting of a pair of numerical values $(E_{2\times1})$, is produced according to the prescribed method described in Eq. (13).

$$\text{if } B = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \text{ and } S = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix}$$

then,

$$E = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} mod 26 = \begin{bmatrix} (s_{11}b_1 + s_{12}b_2) mod 26 \\ (s_{21}b_1 + s_{22}b_2) mod 26 \end{bmatrix} \tag{13}$$

To decipher the ciphertext message E, the receiver must first calculate the key matrix's inverse (S^{-1}), where $S \cdot S^{-1} = I$ and I denotes the identity matrix. Afterward, Eq. (14) can be used to generate the original message.

$$B = S^{-1}.E \text{ mod } 26 \tag{14}$$

5. Deoxyribonucleic acid

Nucleic acids, essential for all forms of life, are bio-polymers composed of nucleotides. DNA and RNA are nucleic acids that differ in the number of bases they contain. DNA consists of nucleotides with four bases, while RNA has three bases. These nucleotides can be represented using two bits of information, which are the combinations 00, 01, 10, and 11. This provides eight possible mappings of these bits to nucleotides, which are detailed in Table 1. These bases have complementary partners, and a sequence of nucleotides can be expressed using symbols. DNA concepts are widely used in computing and data encryption due to their ability to transform binary numbers into nucleotides. The XOR operation on DNA nucleotides is commonly utilized in encryption, as it retrieves the original plaintext during decryption and produces an equal number of 0s and 1s, making it suitable for key scheduling and encryption algorithms in the proposed encryption scheme. Table 2 displays the outcome of applying the XOR operation to all feasible combinations of DNA nucleotides.

6. Hyperchaotic map

The process of rearranging pixel locations in a plain image can be accomplished using the 2D hyper-chaotic map technique, which is founded on a discrete nonlinear dynamic system of 2D hyper-chaos. Eq. (15) shows the mathematical form of the hyperchaotic map [25].

$$\begin{cases} X_{m+1} = a_1 + a_2 * X_m + a_3 r_m \\ r_{m+1} = b_1 + b_2 * X_m^2 \end{cases} \tag{15}$$

where a_1=0.3; a_2=0.4; a_3=0.6; b_1=1.6; b_2=3.8. The system can be generally represented as follows:

$$\left.\begin{aligned} X_{m+1} &= h(X_m, r_m) \\ r_{m+1} &= g(X_m, r_m) \end{aligned}\right\} \tag{16}$$

Where;

$$h(X_m, r_m) = a_1 + a_2 X_m + a_3 X_m^2 + a_4 r_m + a_5 r_m^2 + a_6 X_m r_m, a_i \in \mathbb{Z}, i = 1, 2, \dots, 6$$

$$f(X_m, r_m) = b_1 + b_2 X_m + b_3 X_m^2 + b_4 r_m + b_5 r_m^2 + b_6 X_m r_m, b_i \in \mathbb{Z}, i = 1, 2, \dots, 6$$

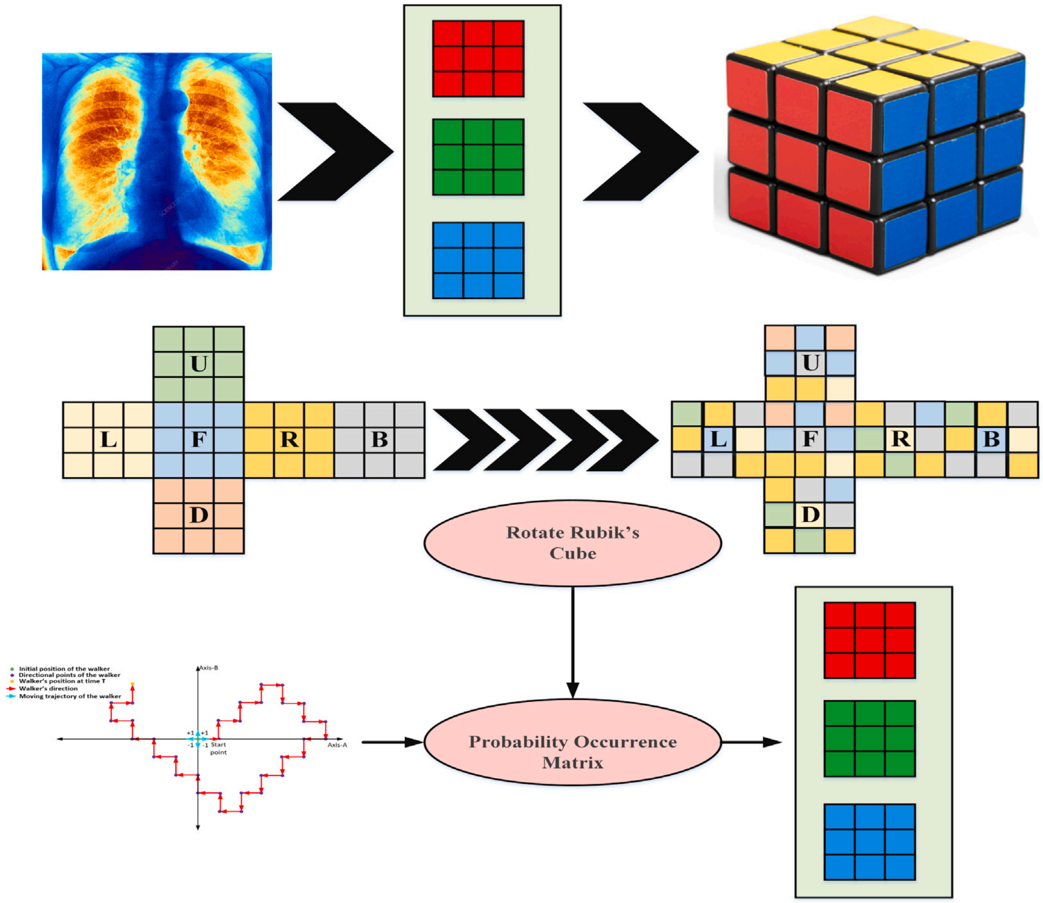

U
L
F
R
B
D
U
L
F
R
B
D
Rotate Rubik's Cube
Initial position of the walker
Directional points of the walker
Walker's position at time T
Walker's direction
Moving trajectory of the walker
Axis-B
Axis-A
+1
+1
-1
-1
Start point
Probability Occurrence Matrix

Fig. 3. Encryption flowchart to create pre-ciphertext image.

The conversion of the Lyapunov exponent of the hyperchaotic system results in (X_m, r_m).

$$\begin{pmatrix} \sigma_{X_{m+1}} \\ \sigma_{r_{m+1}} \end{pmatrix} = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \begin{pmatrix} \sigma_{X_m} \\ \sigma_{r_m} \end{pmatrix}$$

where;

$$g_{11} = \frac{\sigma g}{\partial X} = a_2 + 2a_3 X_m + a_6 r_m; \quad g_{12} = \frac{\partial g}{\partial r} = a_4 + 2a_5 r_m + b_6 X_m;$$
$$g_{21} = \frac{\partial g}{\partial X} = b_2 + 2b_3 A_m + a_6 r_m; \quad g_{22} = \frac{\partial g}{\partial r} = b_4 + 2b_5 r_m + b_6 X_m$$

7. Proposed encryption algorithm

The proposed research involves creating a random matrix via the use of alternating quantum walks, which will then be converted into a 1-D sequence. The Rubik's Cube rotation is controlled by utilizing the 1-D sequence and as a result of this rotation, the scrambling image will undergo XOR with the matrix derived from the random probability matrix to create a pre-ciphertext image. Fig. 3 displays the flowchart for generating the pre-ciphertext image. Subsequently, random sequences are generated utilizing ECC and HC to scramble the pixel rows and columns, resulting in the pre-encrypted image. Finally, the pre-encrypted image will undergo diffusion through DNA encoding and bit-plane extraction. The detailed flow diagram of the proposed encryption scheme is displayed in Fig. 4.

Below are the detailed steps of the encryption algorithm:

1. Load the original color plaintext image (I(m, n)) and split it into three components such as R(m, n), G(m, n), and B(m, n) represented as follows:

   $$I(m, n, 3) = [R(m, n), G(m, n), B(m, n)]$$

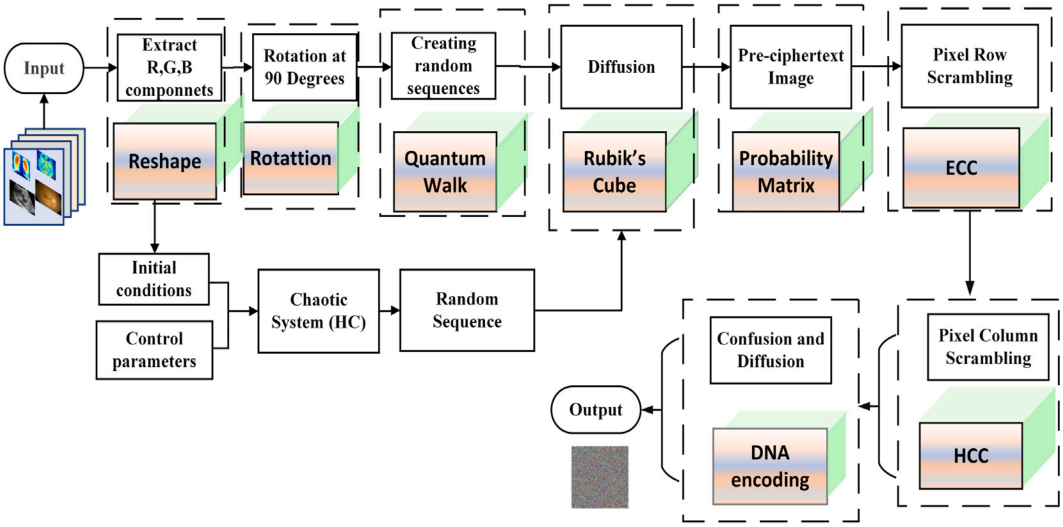


Fig. 4. Complete flow chart for the proposed encryption scheme.

2. Choose the parameters ($M_1, M_2, c\text{and}d$) for the alternate quantum walk, perform the walk for M steps starting from the initial state 0, and create a probability distribution matrix: $P_{B,A}$ with dimensions (m, n) as given in Eq. (17).

$$P_{B,A} = \sum \left| \langle b, a, 0| \bigcup^{M} |\nexists_0 \right|^2 + \sum \left| \langle b, a, 1| \bigcup^{M} |\nexists_0 \right|^2 \tag{17}$$

3. Segment the single-channel image into six distinct sections to yield six separate matrix sub-images. Consider these six matrices as the six faces of an RC namely the front (B), back (E), top (A), bottom (D), left (F), and right (C) sides:

$$I = (B, E, A, D, F, C)$$

4. Extract a 3 × 3 pixel matrix from each of the six matrices to create six different faces, thereby forming a cube of order three. This cube's surface contains 54 pixel values; it has the capacity to generate a cube from the image.
5. Procure the random probability matrix, $P_{b,a}$, using the discrete time alternating quantum walk. Then, transform it into an integer value lies in the range ∈ [017] as given in Eq. (18). This numerical value is utilized to symbolize the rotation method, as depicted in Table 1:

$$T = fix(P_{b,a} \times 10^{16}) mod(18) \tag{18}$$

6. Transform the random matrix $P_{b,a}$ into an integer matrix within the range [0–255] using the expression: $K = fix(P_{b,a} \times 10^{16})$ mod(256). Subsequently, return to step 3 and execute a bitwise XOR operation with the rotated matrix to acquire noisy color components using Eq. (19), (20), and (21).

$$N_{pre-red} = N_{red} \bigoplus K = N_{red} \bigoplus [fix(P_{b,a} \times 10^{16}) mod(256)] \tag{19}$$

$$N_{pre-green} = N_{green} \bigoplus K = N_{green} \bigoplus [fix(P_{b,a} \times 10^{16}) mod(256)] \tag{20}$$

$$N_{pre-blue} = N_{blue} \bigoplus K = N_{blue} \bigoplus [fix(P_{b,a} \times 10^{16}) mod(256)] \tag{21}$$

7. Use Eq. (22) to obtain the color pre-encrypted image.

$$\left.\begin{aligned} N_{pre} &= N_{pre-red}(:, :, 1) \\ N_{pre} &= N_{pre-green}(:, :, 2) \\ N_{pre} &= N_{pre-blue}(:, :, 3) \end{aligned}\right\} \tag{22}$$

8. Now, both the sender and the receiver actively participate in the creation of the secret key matrix (S_m). This identical key will serve the dual purpose of encrypting and decrypting. The N_{pre} will be segmented into blocks, each containing four-pixel values. Thus, each participant generates a 4 × 4 self-invertible key matrix, S_m, employing the method proposed in [26].

Let $S_m = \begin{bmatrix} s_{11} & s_{12} & \vdots & s_{13} & s_{14} \\ s_{21} & s_{22} & \vdots & s_{23} & s_{24} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{13} & s_{32} & \vdots & s_{33} & s_{34} \\ s_{41} & s_{42} & \vdots & s_{43} & s_{44} \end{bmatrix}$ is an invertible matrix partitioned as: $S_m = \begin{bmatrix} S_{11} & \vdots & S_{12} \\ \cdots & \cdots & \cdots \\ S_{21} & \vdots & S_{22} \end{bmatrix}$. The proposed scheme assumes that $S_m = \begin{bmatrix} s_{11} & \vdots & s_{12} \\ \cdots & \cdots & \cdots \\ s_{21} & \vdots & s_{22} \end{bmatrix}$, then, by resolving $S_{12} = I - S_{11}, S_{21} = I + S_{11}$, and $S_{11} + S_{22} = 0$ (Where I represents the identity matrix) the values for the other segments of the secret matrix key Km are determined. Now divide N_{pre} into blocks, each block consisting of four pixel values having the vector size of 4×1 $(N_{pre_1}, N_{pre_2}, N_{pre_3} \cdots N_{pre_n})$. Then, multiply each vector by the invertible key matrix S_m and perform a modulo 256 operation to derive the pre-encrypted vectors $(C_{pen_1}, C_{pen_2}, C_{pen_3}, \dots, C_{pen_n})$. Let $O_1 = \begin{bmatrix} O_{11} \\ O_{21} \\ O_{31} \\ O_{41} \end{bmatrix}$, $C_{en_1} = S_m \cdot O_1 = \begin{bmatrix} s_{11} & s_{12} & s_{13} & s_{14} \\ s_{21} & s_{22} & s_{23} & s_{24} \\ s_{31} & s_{32} & s_{43} & s_{34} \\ s_{41} & s_{42} & s_{43} & s_{44} \end{bmatrix} \cdot \begin{bmatrix} O_{11} \\ O_{21} \\ O_{31} \\ O_{41} \end{bmatrix} =$ $\begin{bmatrix} (s_{11}O_{11} + s_{12}O_{21} + s_{13}O_{31} + s_{14}O_{41}) \text{ mod } (256) \\ (s_{21}O_{11} + s_{22}O_{21} + s_{23}O_{31} + s_{24}O_{41}) \text{ mod } (256) \\ (s_{31}O_{11} + s_{32}O_{21} + s_{33}O_{31} + s_{34}O_{41}) \text{ mod } (256) \\ (s_{41}O_{11} + s_{42}O_{21} + s_{43}O_{31} + s_{44}O_{41}) \text{ mod } (256) \end{bmatrix} = \begin{bmatrix} C_{pen_{11}} \\ C_{pen_{21}} \\ C_{pen_{31}} \\ C_{pen_{41}} \end{bmatrix}$. Similarly, other pre-encrypted vectors $(C_{pen_{i,j}})$ can be obtained as: $S_m \cdot O_2$, $S_m \cdot O_3$, $S_m \cdot O_4 \cdots S_m \cdot O_n$. Following this, reconstruct the pre-encrypted image $C_e n$ using the values from the pre-encrypted vectors.

9. Apply the DNA coding rules as depicted in Tables 1 and 2 to further alter the pre-encrypted image. After that, generate random sequences (R_1 and R_2) using Eq. (13). These sequences are then employed to scramble the pixel rows and columns of the noisy image, which is created after applying the DNA encoding rules, thereby generating the final encrypted image.

8. Simulation results

The primary goal of an encryption algorithm is to ensure that the decrypted image is an exact replica of the original image. To assess the efficiency of the proposed encryption algorithm, analysis, and simulations are conducted on MATLAB 2014 to test the encryption and decryption processes. Moreover, the experimental setup used to test the efficiency of the proposed work, a computer having a specification of 8 GB RAM, windows 11, 512 GB solid-state drive (SSD) and Gen Intel(R) Core(TM) i5-1135G7 @ 2.40 GHz 2.42 GHz.

There are four plaintext medical images, such as a brain tumor image/scan, chest X-ray image, an ultrasound image, and an eye X-ray image, and their corresponding encrypted components encrypted color images, and decrypted images are shown in Fig. 5. By examining the images shown in Fig. 5(e,k,q,w), it becomes evident that the proposed encryption scheme can effectively conceal the plaintext information. Furthermore, the algorithm successfully decrypts and restores the encrypted image without any loss of data (Fig. 5(f,l,r,x)).

9. Statistical analysis

In addition to the simulation results, it is essential to conduct statistical analysis to assess the efficiency of the proposed encryption and decryption algorithms.

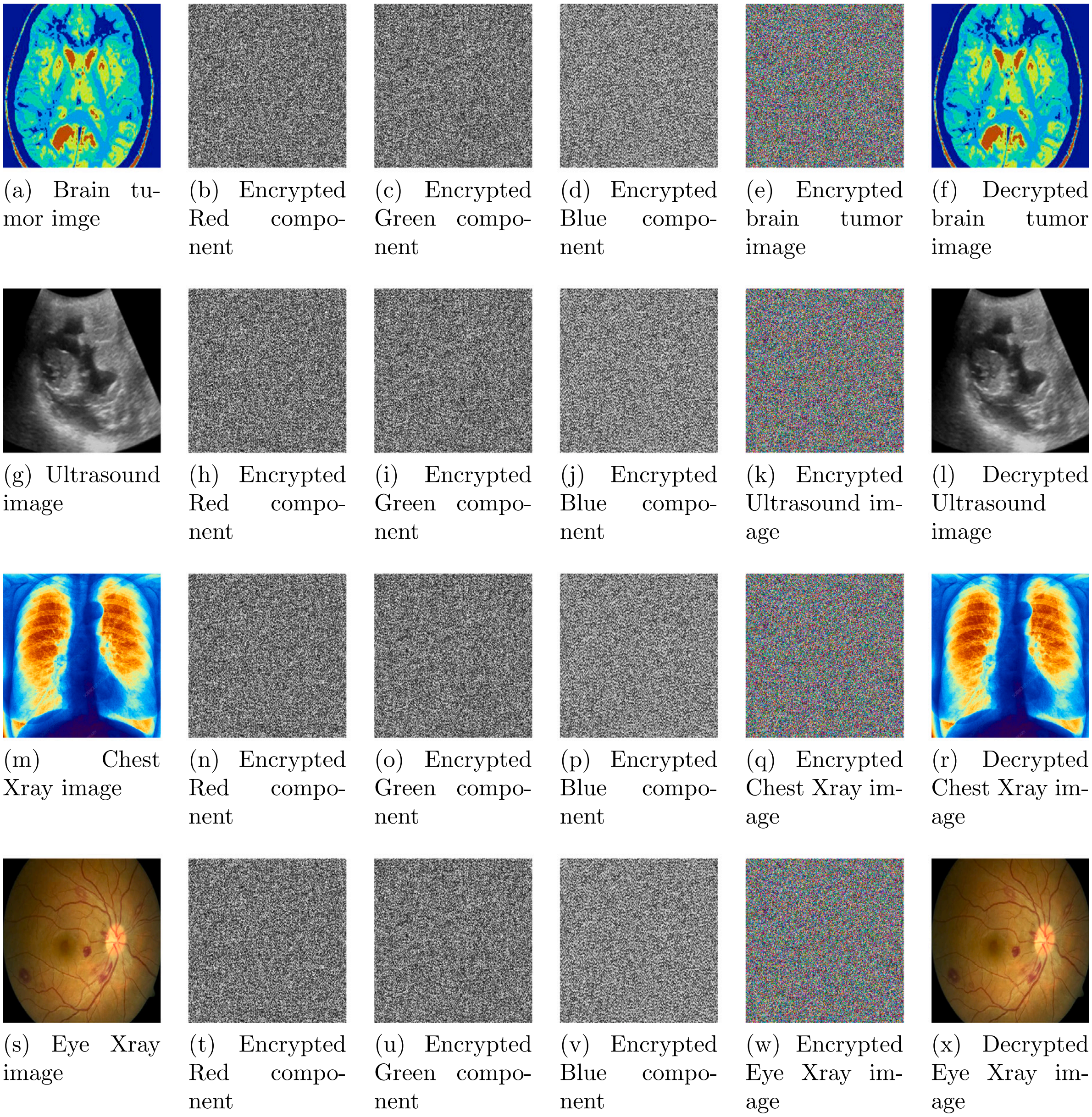
9.1. Key space analysis

The effectiveness of an encryption algorithm in preventing brute force attacks can be enhanced by maximizing the size of its key space. The proposed encryption algorithm's key space consists of various parameters, including $\beta, e_1, e_2, X_m, r_m, a_1, a_2, a_3, b_1$ and b_2 that are contained quantum walk, hill cipher, and hyperchaotic map. By keeping all parameters constant during encryption and adding a tiny change of 10^{-16} during decryption, the resulting decrypted images are uniformly noise-like, as demonstrated in Fig. 6. The key magnitude of the key space of one key can be calculated as (10^{16}). Therefore the total keyspace will be $(10^{16\times 10})$ This value is much larger than the minimum limit of 2^{100}, indicating that the proposed algorithm can effectively withstand brute-force attacks.

9.2. Correlation analysis

Adjacent pixel correlation refers to the extent to which pixels in neighboring locations within a plane image are correlated. Typically, plain images exhibit a high degree of adjacent pixel correlation, whereas cipher images produced through image encryption algorithms should have correlations that are as close to zero as possible. Mathematically, correlation can be calculated as:

$$r_{l,m} = \frac{cov(l, m)}{\sqrt{D(l)}\sqrt{D(m)}} \tag{23}$$



(a) Brain tumor imge

(b) Encrypted Red component

(c) Encrypted Green component

(d) Encrypted Blue component

(e) Encrypted brain tumor image

(f) Decrypted brain tumor image

(g) Ultrasound image

(h) Encrypted Red component

(i) Encrypted Green component

(j) Encrypted Blue component

(k) Encrypted Ultrasound image

(l) Decrypted Ultrasound image

(m) Chest Xray image

(n) Encrypted Red component

(o) Encrypted Green component

(p) Encrypted Blue component

(q) Encrypted Chest Xray image

(r) Decrypted Chest Xray image

(s) Eye Xray image

(t) Encrypted Red component

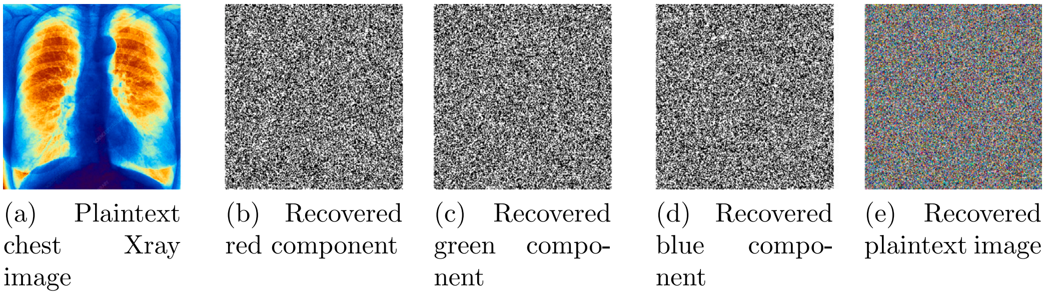
(u) Encrypted Green component

(v) Encrypted Blue component

(w) Encrypted Eye Xray image

(x) Decrypted Eye Xray image

Fig. 5. Plaintext images and their corresponding encrypted components and encrypted color images.



(a) Plaintext chest Xray image

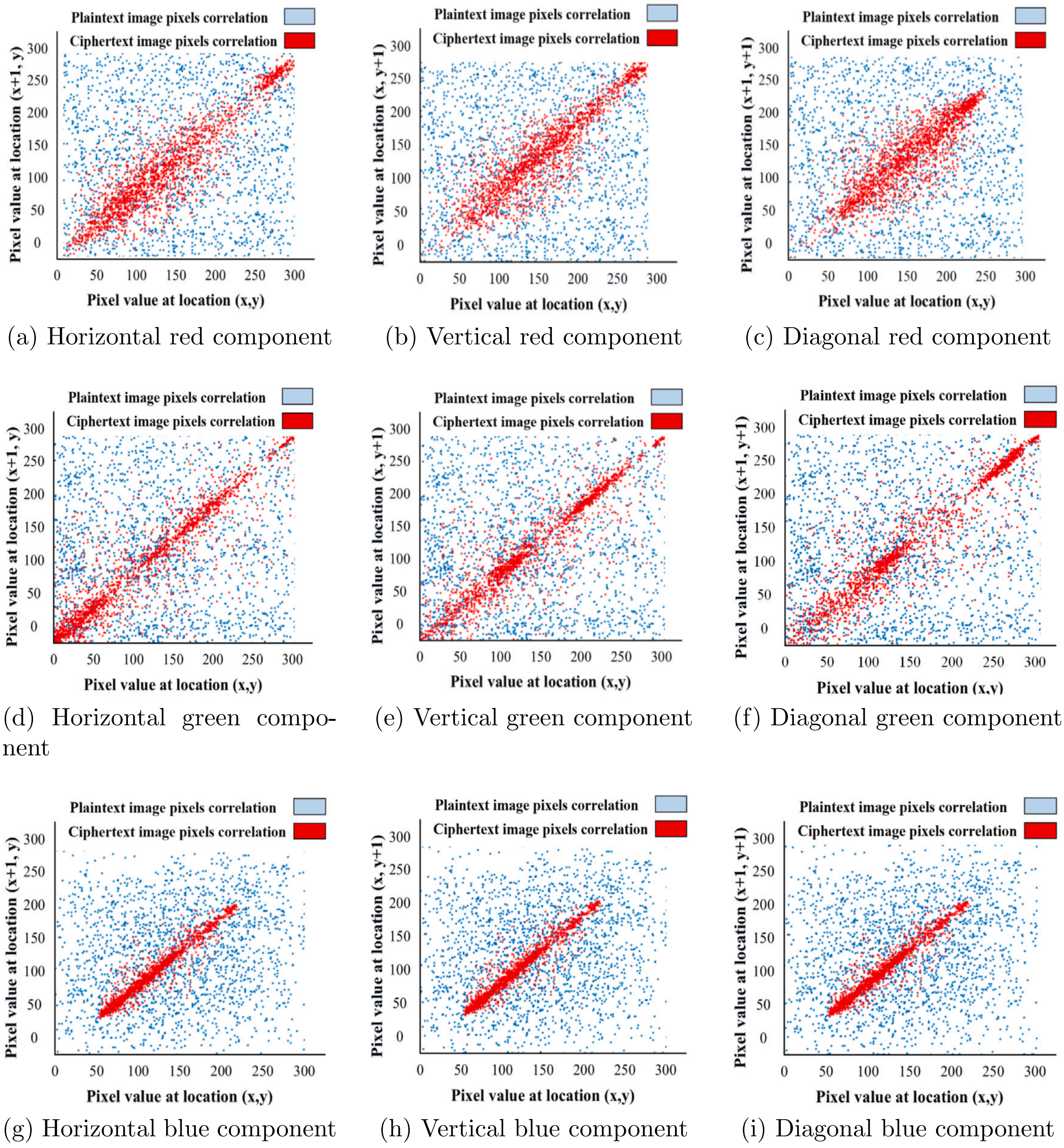
(b) Recovered red component

(c) Recovered green component

(d) Recovered blue component

(e) Recovered plaintext image

Fig. 6. Demonstration of recovering a plaintext image with a tiny change of 10^{-16} in secret keys.



(a) Horizontal red component

(b) Vertical red component

(c) Diagonal red component

(d) Horizontal green component

(e) Vertical green component

(f) Diagonal green component

(g) Horizontal blue component

(h) Vertical blue component

(i) Diagonal blue component

Fig. 7. Pixels scattered diagrams of the plaintext and their corresponding ciphertext images.

Where,

$$D(l) = \frac{1}{M}\sum_{j=1}^{M}(l_j - E(l))^2, \quad cov(l,m) = \frac{1}{M}\sum_{j=1}^{M}(l_j - E(l))(m_j - E(m)),$$

$$E(l) = \frac{1}{M}\sum_{j=1}^{M} l_j$$

l and m denote the gray-scale values of two adjacent pixels within an encrypted image.

In Fig. 7, the correlations of a plaintext image before and after encryption are presented in each direction (horizontal (H), vertical (V), and diagonal (D)). The red and blue dots in the figure represent the pixel scattering of the plaintext and their corresponding ciphertext components, respectively, in all H, V, and D directions. As shown in Fig. 7, the red dots (representing encrypted components) are significantly closer together than the blue dots (representing plaintext components), indicating that the correlation between the encrypted components is lower than that of the plaintext components.

Table 3
Correlation analysis.

Plaintext images	Directions	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	H	0.0042	0.0015	0.0018	0.0021	0.0001
	V	0.0019	0.0041	−0.0321	−0.0056	−0.0013
	D	0.0023	−0.0021	−0.0045	0.0051	−0.0001
Ultrasound	H	0.0027	−0.0035	−0.0023	−0.0043	−0.0018
	V	0.0027	−0.0045	−0.0033	−0.0033	−0.0018
	D	0.0047	−0.0045	−0.0033	−0.0033	−0.0018
Chest Xray	H	0.0027	−0.0035	−0.0043	−0.0033	−0.0021
	V	0.0024	−0.0035	−0.0053	−0.0025	−0.0017
	D	0.0017	−0.0054	−0.0044	−0.0021	−0.0011
Eye Xray	H	0.0017	−0.0034	−0.0024	−0.0033	−0.0024
	V	0.0023	−0.0043	−0.0021	−0.0043	−0.0012
	D	0.0043	−0.0021	−0.0043	−0.0044	−0.0018

Table 4
Entropy analysis.

Plaintext images	Components	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	Red	7.9651	7.9323	7.9760	7.9815	7.9991
	Green	7.9822	7.9813	7.9865	7.9871	7.9990
	Blue	7.9886	7.9881	7.9934	7.9910	7.9990
Ultrasound	Red	7.9431	7.9766	7.9871	7.9984	7.9991
	Green	7.9643	7.9761	7.9843	7.9766	7.9996
	Blue	7.9846	7.9812	7.9811	7.9800	7.9993
Chest Xray	Red	7.9888	7.9846	7.9844	7.9861	7.9991
	7.9986	7.9860	7.9866	7.9984	7.9846	7.9991
	Blue	7.9986	7.9864	7.9844	7.9833	7.9993
Eye Xray	Red	7.9886	7.9886	7.9899	7.9866	7.9993
	Green	7.9984	7.9984	7.9964	7.9866	7.9993
	Blue	7.9864	7.9866	7.9987	7.9798	7.9991

Table 3 presents the correlation coefficient values of the encrypted images. The cipher image exhibits scattered adjacent pixels throughout the rectangular space in all directions, resulting in correlation coefficients that closely approximate ideal values. Furthermore, a comparison with existing encryption schemes, as depicted in Table 3, shows the superiority of the proposed encryption scheme over the existing ones. These results affirm that the proposed encryption scheme successfully disrupts the correlation among adjacent pixels, thereby dismantling the original statistical features of the plain image data.

9.3. Information entropy

Information entropy is frequently used to gauge the amount of information present, and this applies to images as well. A higher information entropy in an image suggests a greater quantity of information, but less visual information. On the other hand, a plain image has more visual information and smaller information entropy. When an image is encrypted, its information entropy should increase significantly compared to the plain image. In fact, the theoretical value for information entropy in such cases is 8, which can be calculated as follows:

$$Entropy = -\sum_{j=0}^{255} \rho(j) log_2 \rho(j) \tag{24}$$

Where $\rho(j)$ represents the probability of occurrence of the gray value j.

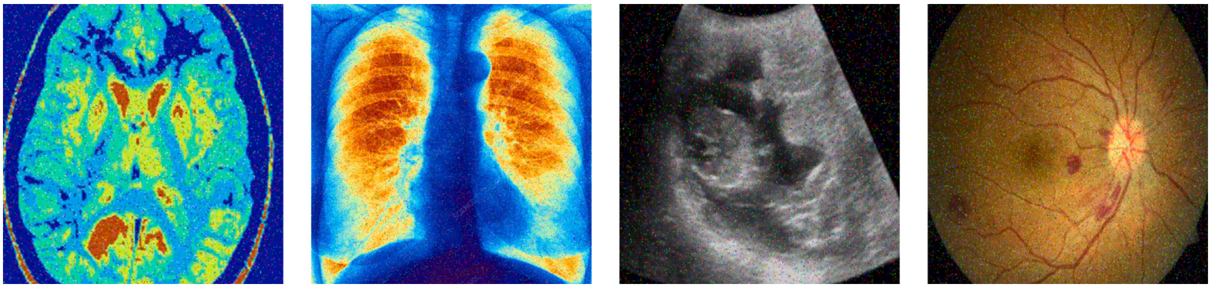
During the experiment, various grayscale plaintext images, including all-black and all-white images, along with their corresponding ciphertext images are used for entropy analysis. The results of this analysis are presented in Table 4. It can be observed that the information entropy of the cipher image experiences a significant increase compared to the plaintext images. Its value can potentially reach up to 7.999, indicating significant proximity to the optimal value. Additionally, Table 12 displays a comparison of the proposed encryption algorithm's test results with those of other encryption schemes. The results show that the proposed encryption algorithm outperforms the other schemes, indicating that it provides better security.

9.4. Noise attack analysis

Images are prone to noise interference during transmission via channels, which can negatively impact their quality. To protect encrypted images from such attacks, robust encryption algorithms are necessary. The effectiveness of an encryption algorithm in

Table 5
Noise attack analysis.

SPN	Components	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
0.07	Red	30.65	30.77	31.64	35.64	45.67
	Green	32.64	34.55	62.87	36.64	45.36
	Blue	41.64	41.67	35.67	39.99	46.97
0.08	Red	39.65	39.46	41.34	41.34	45.66
	Green	39.64	35.48	38.66	39.78	45.66
	Blue	39.64	38.99	41.36	42.65	47.66
0.09	Red	40.64	39.65	38.46	39.99	46.97
	Green	39.65	37.89	39.98	41.65	49.65
	Blue	37.88	38.64	39.44	39.45	49.33
0.10	Red	39.64	38.65	37.64	39.44	46.31
	Green	38.65	39.45	38.77	34.98	46.31
	Blue	38.65	37.65	38.33	38.46	49.63



(a) Recovered brain tumor image when SPN = 0.07

(b) Recovered chest Xray image when SPN = 0.08

(c) Recovered ultrasound image when SPN = 0.09

(d) Recovered eye Xray image when SPN = 0.10

Fig. 8. Noise attack analysis.

defending against noise attacks can be determined by decrypting the encrypted images that is altered using noise, and evaluating the patterns in the decrypted images through the peak signal-to-noise ratio (PSNR). The mathematical form of PSNR is given in Eq. (25),. Whereas, the experimental results are presented in Table 5 and Fig. 8. A higher PSNR value between two images indicates a lesser degree of degradation. The universally accepted PSNR standard is 30 dB, and any images below this threshold are considered to be of poor quality.

$$\begin{cases} MSE = \frac{1}{X \times Y} \sum_{i=0}^{X-1} \sum_{j=0}^{Y-1} \left| P(i,j) - D(i,j) \right| \\ PSNR = 20log_{10}\left(\frac{Max_P}{\sqrt{MSE}} \right) \end{cases} \tag{25}$$

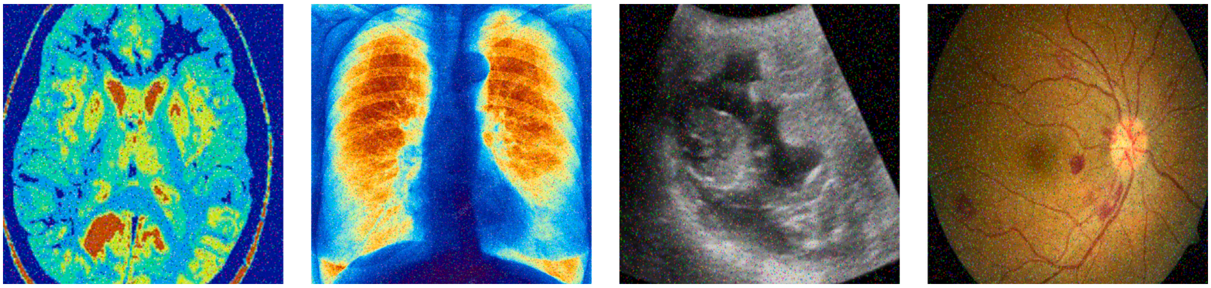
Where $X \times Y$ shows the size of the digital image. $P(I, j)$ and $D(I, j)$ are the plaintext and decrypted images, respectively.

From Table 5, it is evident that the decrypted images maintain a quality of over 40 dB even after being exposed to varying degrees of Salt and Pepper noise (SPN) and Gaussian noise (GN). Additionally, as demonstrated in Fig. 8, the visual information in the decrypted image remains discernible despite being affected by 0.07, 0.08, 0.09, and 0.10 SPN. The results demonstrate the capability of the proposed encryption algorithm to withstand high-amplitude noise attacks.

9.5. Clipping attack

When an attacker modifies a cipher image by replacing specific data with known information, their objective is to manipulate the plaintext image in such a manner that the resulting decrypted image appears intelligible but the actual information conveyed may be incorrect. This attack presents a more rigorous challenge to the encryption process. If a clipping attack leads to an incorrect decryption outcome, it can result in an irreparable loss for both the image sender and receiver.

The encryption algorithm's effectiveness is assessed by subjecting it to rigorous testing against clipping attacks. The decrypted image's quality is evaluated by comparing them with the plaintext image in terms of the percentage of recovered information for various clipping percentage ratios (CPR) such as 7.36%, 13.94%, 16.64%, and 17.53%. The results are displayed in Table 6 and Fig. 9. According to Table 6, more than 90% of the information can be recovered even when the image is cropped by 17.53%. Additionally, Fig. 9 demonstrates that even when the information is clipped by 17.53%, most of the image information remains perceptible. The clipping attack test serves as a complete demonstration of the encryption algorithm's resilience, as it can retrieve a significant portion of the original data despite some data loss.



(a) Recovered brain tumor image when CPR= 7.36

(b) Recovered chest Xray image when CPR= 13.94

(c) Recovered ultrasound image when CPR= 16.64

(d) Recovered eye Xray image when CPR= 17.53

Fig. 9. Clipping attack analysis.

Table 6
Clipping attack analysis.

Clipping percentage	Components	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
7.36%	Red	85.65	89.65	90.64	88.65	96.32
	Green	89.32	89.34	90.46	90.66	96.66
	Blue	89.33	88.19	89.65	90.67	96.49
13.94%	Red	89.67	89.46	90.64	90.64	95.66
	Green	89.45	88.67	88.66	89.19	95.67
	Blue	90.36	89.64	90.67	90.67	95.63
16.64%	Red	89.64	90.64	90.34	91.34	94.66
	Green	89.64	90.64	91.64	92.645	94.96
	Blue	89.34	90.12	89.34	90.64	94.18
17.53%	Red	90.64	91.64	91.66	90.64	93.64
	Green	89.64	90.16	90.45	91.33	93.61
	Blue	90.46	91.66	92.48	91.33	93.10

Table 7
Computational complexity analysis (sec).

Plaintext images (256 × 256 × 3)	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	1.016	0.579	0.646	0.089	0.0001
Ultrasound	0.786	0.866	0.947	0.0742	0.0005
Chest Xray	0.764	0.471	0.848	0.0998	0.0006
Eye Xray	1.075	0.845	0.706	0.037	0.0003

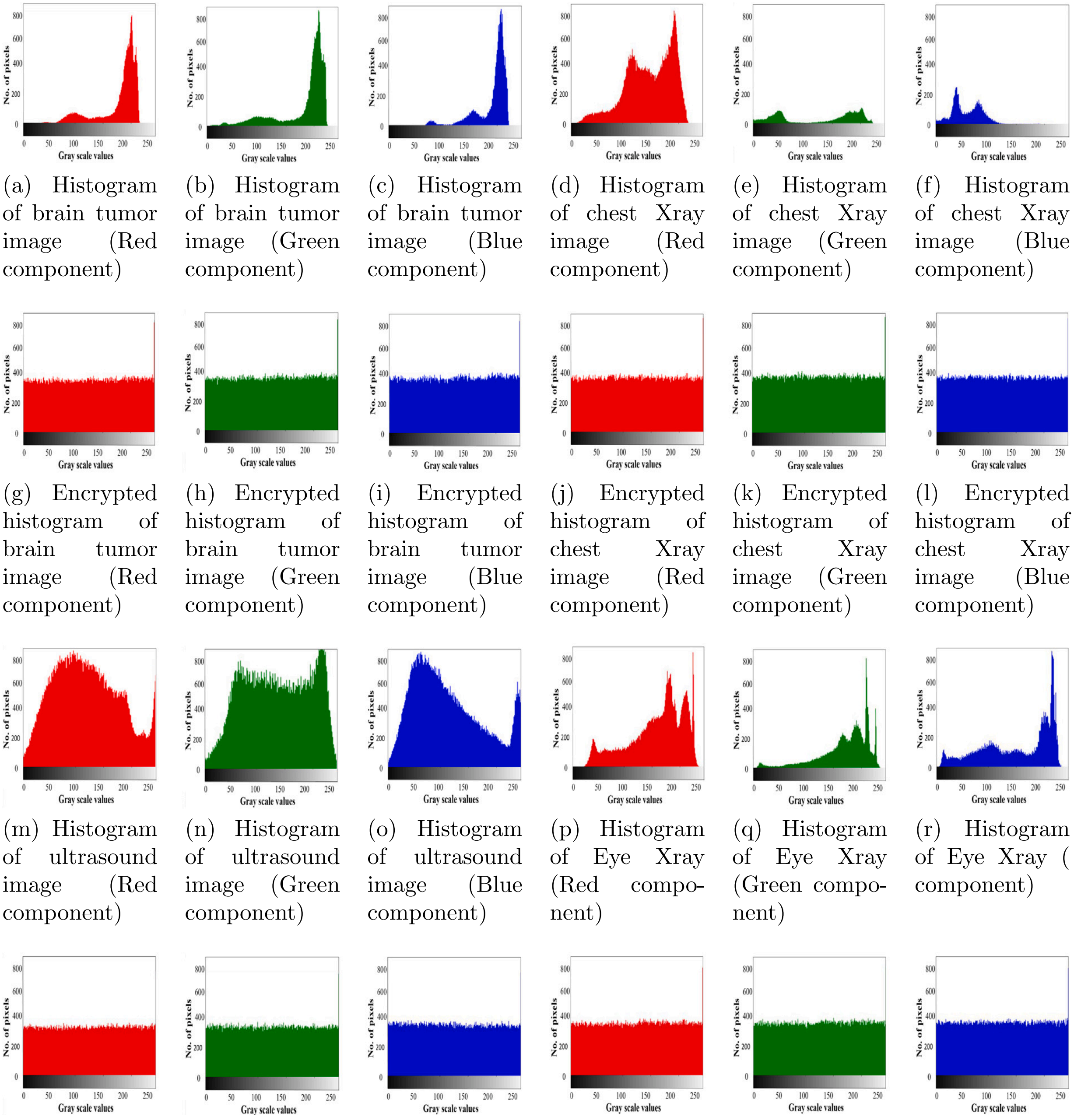
9.6. Computational efficiency analysis

In addition to being highly effective, the encryption algorithm should also be computationally efficient to enable its usage in real-time applications. Usually, the duration for encryption and decryption tends to increase as the size of the image increases. In order to make a comparison with existing algorithms, the average time needed to encrypt a digital image is given in Table 7 which shows that apart from the encryption scheme proposed in [27], the proposed encryption algorithm demonstrates faster performance compared to other similar encryption methods. The encryption scheme presented in [27] only employs confusion and diffusion properties to encrypt a 256 × 256 × 3 color image, leading to lower computational time. However, due to the lesser number of encryption operations, the overall security of the encryption algorithm is not as robust as the proposed encryption scheme.

The proposed encryption scheme integrates various encryption methods, including quantum walks, DNA encoding, and chaotic maps. The implementation of quantum walks and DNA encoding allows for simultaneous confusion and diffusion in the encryption process. By altering both the pixel values and their positions simultaneously during quantum walks, the proposed encryption scheme reduces computational complexity. Furthermore, the size of the final encrypted image remains the same as the original plaintext image, requiring identical storage requirements.

9.7. Histogram analysis

A histogram is a visual way of showing how pixels are distributed within an image. This data is particularly valuable for assessing the effectiveness of encryption methods. A strong encryption technique should produce a histogram for the encrypted image that is uniform and level, with no discernible patterns compared to the original image. To illustrate, Fig. 10 provides a comparison of the



(a) Histogram of brain tumor image (Red component)

(b) Histogram of brain tumor image (Green component)

(c) Histogram of brain tumor image (Blue component)

(d) Histogram of chest Xray image (Red component)

(e) Histogram of chest Xray image (Green component)

(f) Histogram of chest Xray image (Blue component)

(g) Encrypted histogram of brain tumor image (Red component)

(h) Encrypted histogram of brain tumor image (Green component)

(i) Encrypted histogram of brain tumor image (Blue component)

(j) Encrypted histogram of chest Xray image (Red component)

(k) Encrypted histogram of chest Xray image (Green component)

(l) Encrypted histogram of chest Xray image (Blue component)

(m) Histogram of ultrasound image (Red component)

(n) Histogram of ultrasound image (Green component)

(o) Histogram of ultrasound image (Blue component)

(p) Histogram of Eye Xray (Red component)

(q) Histogram of Eye Xray (Green component)

(r) Histogram of Eye Xray (component)

(s) Encrypted histogram of ultrasound image (Red component)

(t) Encrypted histogram of ultrasound image (Green component)

(u) Encrypted histogram of ultrasound image (Blue component)

(v) Encrypted histogram of eye Xray image (Red component)

(w) Encrypted histogram of eye Xray image (Green component)

(x) Encrypted histogram of eye Xray image (Blue component)

Fig. 10. Histogram analysis.

Table 8
Histogram variance analysis.

Plaintext images (256 × 256 × 3)	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	270.654	271.380	269.670	278.140	256.641
Ultrasound	260.640	261.350	270.650	276.981	260.321
Chest Xray	271.306	271.374	272.012	277.633	258.650
Eye Xray	270.644	271.320	277.970	276.820	261.587

Table 9
Maximum deviation analysis.

Plaintext images (256 × 256 × 3)	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	251.221	258.798	249.399	246.533	259.177
Ultrasound	260.623	261.548	270.665	276.977	260.312
Chest Xray	271.361	271.367	272.094	277.698	258.621
Eye Xray	270.641	271.363	277.977	276.821	261.578

histograms for the R, G, and B components of the plaintext image and the corresponding component of the encrypted image. The histogram for the encrypted image displays a uniform distribution of pixels and is distinct from the original image's histogram with no recognizable patterns. This indicates that the encryption method proposed can withstand statistical cyberattack attacks.

9.8. Histogram variance analysis

Variance serves as an additional parameter for assessing the histogram's uniformity in the enciphered images. This metric provides statistical values rather than histogram visualization. Eq. (26) shows the calculation of variance.

$$Var(G) = \frac{1}{256}\sum_{K=1}^{256}[g_i - E(G)]^2 \tag{26}$$

Where G is the stream of pixels, $G = \{\ g_1, g_2, g_3 \ldots, g_{256}, g_i\}$ is the pixel value at Kth position and $C(G) = \frac{1}{256}\sum_{K=1}^{256} g_i$. In order to achieve strong encryption, it is desirable to have low variance values. Table 8 presents a comparison of variance values obtained from the enciphered images generated by both the proposed and existing encryption schemes. The results indicate that the proposed scheme outperforms the existing ones, as evidenced by the lower variance values.

9.9. Maximum deviation

The quality of a cryptographic algorithm can be assessed based on the disparity in pixel values between the plaintext and ciphertext images. A higher deviation in pixel changes signifies a more robust encryption technique in terms of security. The mathematical expression for the maximum deviation is represented by Eq. (27).

$$D_m = \frac{A_0 + A_{G-1}}{2} + \sum_{K=1}^{G-2} A_K \tag{27}$$

Where G represents the number of gray levels, while A_K denotes the amplitude of the difference histogram at index K. A higher value of "D" indicates a significant dissimilarity between the enciphered and the original image. The results of the maximum deviation for both the proposed method and the existing algorithms are presented in Table 9. Through a comparison of the average maximum deviations, it is evident that the proposed encryption algorithm exhibits superior performance compared to other similar schemes. These findings suggest that the maximum deviations observed in the proposed method do not disclose any significant information about the quality of the encryption.

9.10. Irregular deviation

To evaluate the encryption quality, relying solely on the maximum deviation (M_D) is insufficient. Another metric, denoted as I_D, is utilized to assess the quality of the enciphered image by measuring the statistical distribution of deviations between the original and encrypted images to a uniform statistical distribution. The calculation of I_D is given in Eq. (28).

$$D_I = \sum_{K=0}^{G-1} |B_L - A_H| \tag{28}$$

In the equation, B_L represents the peak of the histogram at position K, and A_H represents the average sum of the histogram values. A lower value of D_I indicates better quality of the encrypted image. The values of D_I for both the proposed and existing encryption schemes are presented in Table 10. It can be observed that the proposed encryption method exhibits lower D_I values compared to the existing schemes, indicating its stronger security and superior performance in comparison to others.

Table 10
Irregular deviation analysis.

Plaintext images ($256 \times 256 \times 3$)	Ref. [27]	Ref. [28]	Ref. [29]	Ref. [30]	Proposed
Brain tumor	46848	47645	48551	47313	450329
Ultrasound	45570	46997	47888	46691	45071
Chest Xray	46616	47612	47135	49970	45671
Eye Xray	46787	46646	47664	46644	45340

10. Challenges and possible solution

While designing the proposed encryption scheme for medical images, several challenges are faced which are outlined below along with their potential ways to overcome.

10.1. Computational complexity

In addition to robust security, computational efficiency is a vital aspect of any image encryption scheme. The proposed encryption scheme combines various encryption methods, including DNA, quantum walk, and chaos. However, the execution time increases due to the involvement of multiple methods and mathematical steps required to achieve the encrypted image.

In order to ensure the computational efficiency of the encryption scheme, the confusion and diffusion operations are performed in parallel by employing both quantum walk and DNA operations simultaneously, rather than sequentially. This approach significantly reduces the processing time needed for encrypting the plaintext image.

10.2. Key management

During the design of the proposed encryption schemes, a significant challenge arises from the fact that the key space is relatively small, measuring less than 2^{100}. This limited key space makes the scheme vulnerable to brute force attacks, as an attacker can easily try all possible combinations of secret keys.

To address this challenge, ten secret keys are employed to encrypt the plaintext image. Each individual key possesses a considerably larger keyspace, exceeding 2^{45} as stated in Section 9.1. By combining the keyspace of all ten keys, the resulting keyspace surpasses 2^{100}, providing robust protection against brute force attacks.

10.3. Compatibility and interoperability

The encryption scheme may encounter the challenge of being incompatible with various formats, including JPG and PNG. JPG files, for example, utilize lossy compression techniques that can result in a loss of quality when decrypted.

To overcome this challenge, the proposed encryption scheme ensures seamless decryption of the plaintext image without any pixel disruption. This ensures that the encryption scheme is applicable to images of different formats, maintaining the integrity of the decrypted image.

11. Conclusion

The proposed research presents a new encryption method for color medical images that incorporates several advanced cryptographic techniques, including alternate quantum walks, RC, ECC with hill ciphers, and DNA encoding. The proposed encryption algorithm involves generating a random sequence through a quantum random walk and then extracting image pixels to form a third-order RC. The RC is rotated using the generated random sequence to create a scrambled image, which is further enhanced using ECC with the standard Hill cipher algorithm. An encryption or decryption key is produced using the ECC approach, resulting in a robust secret key that does not require sharing over the internet, thus providing better security. An invertible key matrix is utilized for encryption and decryption, eliminating the need to find the inverse key matrix during decryption. Multiple images are arranged and combined into a 3D cube, which undergoes various operations such as rotation, DNA addition, and position swapping to generate the final cipher image. The simulation results of the encryption process for different images indicate that this algorithm is suitable for images that contain highly correlated data as well as those that do not, of any number and size. By analyzing the statistical properties, it is evident that this proposed encryption method can eliminate the correlation between adjacent pixels in the original image, leading to a uniform distribution of image pixels. Consequently, the algorithm can efficiently conceal the original image information, significantly enhancing the encryption's security. Moreover, the large key space of the algorithm offers robust security against exhaustive search attacks. Differential attack assessments and durability tests demonstrate that the encryption technique can withstand such attacks and tolerate a degree of data loss or noise injection. Additionally, the evaluation of computation time indicates that the proposed encryption method is well-suited for real-time applications, due to its minimized encryption processing time. Future research will concentrate on identifying more effective methods to improve the security and efficiency of the suggested encryption algorithm, as well as reduce the time needed for encryption, and boost the algorithm's overall performance speed.

Declaration of competing interest

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript. The authors declare no conflicts of interests.

Data availability

No data was used for the research described in the article.

References

[1] V. Pavithra, J. Chandrasekaran, Developing security solutions for telemedicine applications: Medical image encryption and watermarking, in: Research Anthology on Telemedicine Efficacy, Adoption, and Impact on Healthcare Delivery, IGI Global, 2021, pp. 612–631.
[2] M.K. Hasan, T.M. Ghazal, R.A. Saeed, B. Pandey, H. Gohel, A. Eshmawi, S. Abdel-Khalek, H.M. Alkhassawneh, A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things, IET Commun. 16 (5) (2022) 421–432.
[3] A. Belazi, S. Kharbech, M.N. Aslam, M. Talha, W. Xiang, A.M. Iliyasu, A.A. Abd El-Latif, Improved Sine-Tangent chaotic map with application in medical images encryption, J. Inform. Secur. Appl. 66 (2022) 103131.
[4] S. Kumar, B. Panna, R.K. Jha, Medical image encryption using fractional discrete cosine transform with chaotic function, Med. Biol. Eng. Comput. 57 (2019) 2517–2533.
[5] F. Ahmed, M.U. Rehman, J. Ahmad, M.S. Khan, W. Boulila, G. Srivastava, J.C.-W. Lin, W.J. Buchanan, A DNA based colour image encryption scheme using a convolutional autoencoder, ACM Trans. Multimedia Comput. Commun. Appl. 19 (3s) (2023) 1–21.
[6] M.B. Salunke, P.N. Mahalle, G.R. Shinde, Rubik's cube encryption algorithm-based technique for information hiding during data transmission in sensor-based networks, Int. J. Intell. Syst. Appl. Eng. 10 (1s) (2022) 429–439.
[7] L. Zhang, X. Tian, S. Xia, A scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence, in: 2011 International Conference on Multimedia and Signal Processing. Vol. 1, IEEE, 2011, pp. 312–315.
[8] K. Loukhaoukha, J.-Y. Chouinard, A. Berdai, A secure image encryption algorithm based on Rubik's cube principle, J. Electr. Comput. Eng. 2012 (2012) 7.
[9] R. Vidhya, M. Brindha, A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF), J. King Saud Univ.-Comput. Inf. Sci. 34 (5) (2022) 2000–2016.
[10] I. Ismail, M. Amin, H. Diab, How to repair the Hill cipher, J. Zhejiang Univ.-Sci. A 7 (2006) 2022–2030.
[11] B. Acharya, S.K. Panigrahy, S.K. Patra, G. Panda, Image encryption using advanced hill cipher algorithm, Int. J. Recent Trends Eng. 1 (1) (2009) 663–667.
[12] G. Hamissa, A. Sarhan, H. Abdelkader, M. Fahmy, Securing JPEG architecture based on enhanced chaotic hill cipher algorithm, in: The 2011 International Conference on Computer Engineering & Systems, IEEE, 2011, pp. 260–266.
[13] N.K. SK, S.K. HS, H. Panduranga, Encryption approach for images using bits rotation reversal and extended hill cipher techniques, Int. J. Comput. Appl. 59 (16) (2012).
[14] M.N.A. Rahman, A. Abidin, M.K. Yusof, N. Usop, Cryptography: A new approach of classical hill cipher, Int. J. Secur. Appl. 7 (2) (2013) 179–190.
[15] K. Agrawal, A. Gera, Elliptic curve cryptography with hill cipher generation for secure text cryptosystem, Int. J. Comput. Appl. 106 (1) (2014).
[16] Z. Tang, J. Song, X. Zhang, R. Sun, Multiple-image encryption with bit-plane decomposition and chaotic maps, Opt. Lasers Eng. 80 (2016) 1–11.
[17] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, H. Huang, Cross-plane colour image encryption using a two-dimensional logistic tent modular map, Inform. Sci. 546 (2021) 1063–1083.
[18] H.-S. Ye, N.-R. Zhou, L.-H. Gong, Multi-image compression-encryption scheme based on quaternion discrete fractional Hartley transform and improved pixel adaptive diffusion, Signal Process. 175 (2020) 107652.
[19] R. Enayatifar, F.G. Guimarães, P. Siarry, Index-based permutation-diffusion in multiple-image encryption using DNA sequence, Opt. Lasers Eng. 115 (2019) 131–140.
[20] Y. Gao, S. Jiao, J. Fang, T. Lei, Z. Xie, X. Yuan, Multiple-image encryption and hiding with an optical diffractive neural network, Opt. Commun. 463 (2020) 125476.
[21] A. Sahasrabuddhe, D.S. Laiphrakpam, Multiple images encryption based on 3D scrambling and hyper-chaotic system, Inform. Sci. 550 (2021) 252–267.
[22] A. El-Latif, A. Ahmed, B. Abd-El-Atty, M. Amin, A.M. Iliyasu, Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications, Sci. Rep. 10 (1) (2020) 1–16.
[23] G. Ye, M. Liu, M. Wu, Double image encryption algorithm based on compressive sensing and elliptic curve, Alex. Eng. J. 61 (9) (2022) 6785–6795.
[24] M.A. Lone, S. Qureshi, RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher, Optik 260 (2022) 168880.
[25] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, X. Chen, An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map, J. King Saud Univ.-Comput. Inf. Sci. 34 (4) (2022) 1535–1551.
[26] B. Acharya, G.S. Rath, S.K. Patra, S.K. Panigrahy, Novel methods of generating self-invertible matrix for hill cipher algorithm, 2007.
[27] S.T. Kamal, K.M. Hosny, T.M. Elgindy, M.M. Darwish, M.M. Fouda, A new image encryption algorithm for grey and color medical images, IEEE Access 9 (2021) 37855–37865.
[28] W. El-Shafai, E.E.-D. Hemdan, Robust and efficient multi-level security framework for color medical images in telehealthcare services, J. Ambient Intell. Humaniz. Comput. (2021) 1–16.
[29] S. Deb, B. Bhuyan, Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR, Multimedia Tools Appl. 80 (2021) 19803–19826.
[30] S. Wang, Q. Peng, B. Du, Chaotic color image encryption based on 4D chaotic maps and DNA sequence, Opt. Laser Technol. 148 (2022) 107753.