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]*Department of Computer Science, University of Sunderland, UK*

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.

Keywords: Medical image encryption, quantum cryptography, DNA encoding, color image

encryption, multilayered encryption

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 sen-

sors, 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 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 zeroes. 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 decrytping 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 zeroes. 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 o ers 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 e cient 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 e ectiveness 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 (H^C) and rambler's space (H^L). As a result, the quantum walk may be represented within the Hilbert space denoted as $H = H^C \quad H^L$, where 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 rst stage, the coin operator is applied to the coin state within H^C. The second stage involves the application of the unitary operator $S()$ to the complete H. Therefore, the quantum walk can be perceived as the iterative application of the unitary operator on the quantum walk system. Mathematically, the operator $\hat{S}$ can be expressed as given in Equation 1.

$$[\hat{\ } = T\,O = T(\hat{O} \quad I) \tag{1}$$

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

$$\hat{O} = \begin{matrix} \cos & \sin \\ \sin & \cos \end{matrix} \tag{2}$$

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

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

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

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

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

The alternate quantum walk operates in a two-dimensional space where the position state tensor $\{|A;B;a;b\rangle \in Z\}$ 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 Equations 5, 6, and 7:

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

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

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

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 Figure 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 $|coin\rangle = x|0\rangle + y|1\rangle$, the quantum walk's starting state can be expressed as $|\Psi_0\rangle = |00\rangle \otimes |coin\rangle$. Upon completing N steps, the quantum state of the whole system is represented as $|\Psi_N\rangle = \hat{U}^M |\Psi_0\rangle$, and the mathematical form for the probability of locating the walker at position $(y;x)$ is provided in Equation 8. Algorithm 1 outlines the procedure for employing quantum walk in the proposed encryption algorithm.

$$P_{X;Y} = \sum_{y;x;0} \left|\langle \hat{U}^M \Psi_0 \rangle\right|^2 + \sum_{y;x;1} \left|\langle \hat{U}^M \Psi_0 \rangle\right|^2 \tag{8}$$

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 di erent.

To solve a 3rd-order RC, the arrangement of the six faces and the identi cation of each sub-block must be established. The expansion map for a 3rd-order RC is shown in Figure 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 rst layer of the A side by 90^0 to the right, the resulting state of the Cube is demonstrated in Figure 2.

Figure 1: Quantum walk

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.

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 shu ed using a speci c 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 con dentiality 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 Equation 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,

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((NoOfStates +1)/2) = 1;
! Define the coin operator/space H^C
! Apply Hadmard coin as follows:
    H = 1/√2 [1 1; 1 -1];
! The Hadamard coin maps the basis states |0i and |1i to an equal superposition of the two states

    H|0i = 1/√2 (|0i + |1i)

    H|1i = 1/√2 (|0i - |1i)
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 * 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
```

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

$$a_3 = (R^2 - a_1 - b_2)(\text{mod}P)$$

$$b_3 = (Ra_1 - Ra_3 - b_1)(\text{mod}P)$$

4.2. Point doubling

When a point $P = (a_1; b_1)$ on the elliptic curve E is added to itself, it is referred to as "point doubling" as given in Equation 10. The outcome of doubling point P is point T, which is also situated