scientific reports

Check for updates

OPEN

Cascading quantum walks with Chebyshev map for designing a robust medical image encryption algorithm

Fahad Alblehai[1,7], Ahmed A. Abd El-Latif[2,3,7]✉, Paweł Pławiak[4,5,7] & Bassem Abd-El-Atty[6,7]✉

The secure storage and transmission of healthcare data have become a critical concern due to their increasing use in the diagnosis and treatment of various diseases. Medical images contain confidential patient information, and unauthorized access to or modification of these images can have severe consequences. Chaotic maps are commonly used for constructing medical image cipher systems, but with the growth of quantum technology, these systems may become vulnerable. To address this issue, a new medical image cipher algorithm based on cascading quantum walk with Chebyshev map has been presented in this paper. The proposed system has been tested and found to have high levels of security and efficiency, with UACI, NPCR, Chi-square, and global information entropy values averaging at 33.48095%, 99.62984%, 248.92128, and 7.99923, respectively.

Medical multimedia plays a vital role in modern healthcare by providing a non-invasive method of diagnosing and visualizing various medical conditions for clinicians and researchers. Medical images are generated using different imaging modalities such as PET scans, ultrasound, CT scans, X-rays, and MRI scans. These images offer valuable information about the human body's structure and function, enabling the diagnosis and monitoring of various diseases and conditions, including heart disease, cancer, neurological disorders, and musculoskeletal injuries[1,2].

However, the transmission and storage of medical images pose significant challenges due to the sensitive information they contain. Medical images often include personal information such as patient names, medical histories, and dates of birth, making them an attractive target for cybercriminals and other malicious actors[3,4]. To address these challenges, researchers have developed various security techniques to protect the confidentiality of medical images during transmission and storage. These techniques include image encryption and image data hiding[5–7]. Image encryption techniques aim to convert the image from a readable form into a coded form that is unreadable without the decryption key.

Developing new and more effective medical image cipher algorithms is critical to ensuring the security and confidentiality of medical images and maintaining patient trust in the healthcare system. Chaotic maps are increasingly being used in medical image cipher systems due to their ability to produce high levels of randomness and nonlinearity, making them difficult to predict. The healthcare industry is increasingly concerned about the potential of quantum computers hacking into medical cryptosystems. With the potential to break current cipher algorithms that safeguard sensitive medical information, such as patient records and medical images, the compromise of patient data could have severe consequences for patient privacy and healthcare providers. Therefore, some researchers pay attention to developing quantum cipher systems for securing medical images in the quantum era.

Although researchers are working on designing quantum cipher techniques that are resistant to quantum attacks, it may take several years before they become widely adopted. In the meantime, healthcare providers must take steps to protect their sensitive medical information from quantum attacks by implementing additional

[1]Computer Science Department, Community College, King Saud University, 11437 Riyadh, Saudi Arabia. [2]Jadara University Research Center, Jadara University, Irbid, Jordan. [3]Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt. [4]Department of Computer Science, Faculty of Computer Science and Telecommunications, Cracow University of Technology, Warszawska 24, 31-155 Krakow, Poland. [5]Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland. [6]Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt. [7]Fahad Alblehai, Ahmed A. Abd El-Latif, Paweł Pławiak and Bassem Abd-El-Atty contributed equally to this work. ✉email: a.rahiem@gmail.com; bassem.abdelatty@fci.luxor.edu.eg

security measures and closely monitoring their systems for any signs of unauthorized access or activity. Hence, certain scholars are focusing on developing novel cryptosystems that rely on quantum models and can be implemented on digital devices, not just quantum computers, and possess the adequate capability to withstand quantum attacks during the quantum age[8–10]. For example, Abd-El-Atty[11] developed a color image cipher approach using a logistic-sine map and quantum walks. This approach combines the probability distribution produced from quantum walk with the chaotic stream generated from the chaotic map using quaternions. In[5], Abd-El-Atty et al. developed a double medical image cipher algorithm using a logistic map and quantum walks. This approach splits two medical images into low and high 4-bit images, with the high 4-bit image being ciphered with quantum walks. The chaotic sequences produced by the chaotic systems in[5,8–12] do not rely on the running of quantum walks. Instead, these sequences are generated separately from the chaotic systems and quantum walks and then combined using quaternion[11], adapted particle swarm optimization[8,9], or summation processes[5,10].

Therefore, we need to develop a novel medical image cipher technique based on a quantum paradigm and a chaotic map in which the chaotic sequence produced from the chaotic mapping relies on the running of quantum walks and the pristine image, besides its initial conditions and control parameters. In this study, a new medical image cipher mechanism based on cascading quantum walk with Chebyshev map is proposed. To fulfill a high sensitivity of the plain image for the presented cipher mechanism, the hashing algorithm SHA256 is executed on the plain medical image, and the resulting hash value is utilized to update initial parameters. By using these updated parameters, we act quantum walks to produce a probability distribution vector, which is then used along with the updated initial condition to iterate the Chebyshev map and produce a chaotic sequence that relies on quantum walks and the pristine image. This sequence is used for the confusion phase of the pristine image, as well as for ciphering the blocks of the confused image and performing the diffusion phase for the ciphered blocks. Our simulation outcomes and numerical analyses have demonstrated that this cipher mechanism is both secure and highly efficient.

The original contributions of this study can be highlighted as listed below:

1. Designing an efficient medical image cipher technique based on cascading quantum walks with Chebyshev map, as demonstrated by simulation results and numerical analyses.
2. Opening the way for cascading quantum models with chaotic maps for developing modern cipher systems that possess the adequate capability to withstand quantum attacks during the quantum age.
3. The produced chaotic stream from the cascading system relies on the running of quantum walks and it is related to the pristine image.
4. The simulation outcomes and numerical analyses demonstrate that this cipher mechanism is both secure and highly efficient.The remains of this study are outlined as follows: "Related works" stated the related works of this study, while "Preliminaries" displays the preliminary knowledge of the Chebyshev map and quantum walks. The proposed medical image cipher algorithm is presented in "Proposed cipher mechanism", while its experimental results are displayed in "Experimental results and analyses". Finally, "Conclusion and futur works" stated conclusions drawn from this work.

Related works

With the increasing reliance on digital storage and transmission of sensitive medical information, ensuring the security of medical images has become a critical concern. While traditional encryption methods such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) offer robust security, they may not be well-suited to medical images' complex, high-dimensional nature[13]. To address these challenges, researchers have increasingly explored chaotic maps as a promising solution for medical image encryption, leveraging their distinct security properties, including randomness, sensitivity to initial conditions, and non-linearity.

Chaotic maps are particularly effective for encrypting intricate data like medical images due to their sensitivity to initial conditions, unpredictability, and ergodicity. The encryption process using chaotic maps typically involves two key steps: permutation and diffusion. Permutation rearranges the pixel positions of the image based on chaotic sequences, while diffusion modifies pixel intensities, creating a highly nonlinear and unpredictable relationship between the original and encrypted images. These combined processes offer significant resistance to common cryptographic attacks, such as brute force, differential, and statistical attacks, ensuring the security of medical images during both transmission and storage.

Numerous encryption schemes based on various chaotic maps have been proposed for medical image encryption, each offering distinct advantages in terms of encryption strength, computational efficiency, and resistance to attacks. For example, El-Shafai et al.[14] employed a PWLC map, logistic map, and DNA encoding for designing a medical image cipher approach, which consumes extra processing time due to extra intermediate image operations. In[15], Abdelfatah et al. designed a medical image cipher approach for WBAN based on multi-chaotic maps and DNA encoding, in which the presented approach consists of one round of diffusion and there is no confusion phase for resisting occlusion attacks. Using DNA encoding and a new hybrid chaotic system, Guesmi and Farah[16] designed a medical image cipher approach in which the encrypted medical image is created after iterating the cipher algorithm 10 times. Based on DNA encoding and three chaotic systems, Dagadu et al.[17] designed a medical image cipher approach in which the presented approach consists of two phases (DNA diffusion and key generation) and there is no confusion phase. Liu et al.[18] introduced a new spatiotemporal chaos model and demonstrated its application in developing a new encryption scheme to protect multiple medical images. The encryption scheme includes pixel blurring, asymmetric DNA encoding and decoding, a new DNA operation, and 3D-Fisher scrambling. Nevertheless, DNA encoding and decoding operations are computationally intensive, especially for high-resolution images, making the scheme less efficient in terms of speed and performance.

In[19], Jain et al. incorporate two chaotic systems for designing a medical image cipher approach, which consumes two rounds of substitution and permutation procedures for generating the final ciphered image. Using an enhanced Sine-Tangent chaotic system, Belazi et al.[20] presented a new cryptosystem for securing medical images whereas the cipher approach consists of one confusion phase and two diffusion phases. Based on a new hyperchaotic map, Lai et al.[21] developed a medical image cipher approach in which the presented approach consists of two diffusion phases and one confusion phase. Nevertheless, this approach[21] suffers from plain image sensitivity attacks due to the fact that the generated key streams from the hyperchaotic system are not associated with the original image. In[22], Masood et al. designed a medical image cipher approach based on Chen's chaotic map, Brownian motion and, Henon map, in which this approach is suitable only for gray scale images of dimension 512×512 and the generated key streams from chaotic systems are not related to the pristine image. Also, Kamal et al.[23] proposed a new medical encryption algorithm for encrypting both grey and color images. It consists of four main steps: image splitting, image scrambling, key generation based on a chaotic logistic map, and image diffusion. Nevertheless, this approach is appropriate only for encrypting medical images with specific sizes and suffers from plain image sensitivity attacks due to the fact that the generated key streams from the hyperchaotic system are weakly associated with the original image. Zhuang et al.[24] presented a new medical image encryption approach based on QR decomposition and a 5-dimensional multi-band multi-wing chaotic map. Nevertheless, this approach suffers from plain image sensitivity attacks because the generated key streams from the chaotic system are not associated with the original image. Zhang et al.[25] introduced a novel hyperchaotic system and demonstrated its application in developing a new medical image encryption algorithm. The algorithm employs a novel dynamic Josephus scrambling technique based on chaotic sequences to scramble the image pixel positions, and a dynamic parallel cross-diffusion scheme combined with chaotic sequences to further encrypt the scrambled image. The initial key of the algorithm is updated using the generated hash value from the SHA-256 algorithm for the original image.

The healthcare industry is increasingly concerned about the potential of quantum computers hacking into medical cryptosystems. With the potential to break current cipher algorithms that safeguard sensitive medical information, such as patient records and medical images, the compromise of patient data could have severe consequences for patient privacy and healthcare providers. Therefore, some researchers pay attention to developing quantum cipher systems for securing medical images in the quantum era. For example, El-Latif et al.[26] developed a quantum medical image cipher algorithm based on a logistic-sine map and gray code. This approach involves two phases, key generation and diffusion, but does not include a confusion phase. In[27], Aparna et al. presented a quantum medical image cipher approach using an integration of two chaotic systems in which the generated key streams from the combined chaotic systems are not associated with the original image. Prajapat et al.[28] introduced a quantum image encryption protocol that leverages chaotic maps and gray coding techniques to encrypt grayscale medical images. This approach involves two phases, key generation and diffusion, but does not include a confusion phase. Also, the generated chaotic sequence from the chaotic map is not associated with the original image. Kadhim and Atia[29] introduced a quantum image encryption protocol that leverages a 9-dimensional chaotic map to encrypt both grayscale and color medical images. This approach employs quantum logic for image scrambling, integrating it with the encryption key through the C-NOT quantum gate. Nevertheless, the generated chaotic sequence from the chaotic map is not associated with the original image.

Although researchers are working on designing quantum cipher techniques that are resistant to quantum attacks, it may take several years before they become widely adopted. In the meantime, healthcare providers must take steps to protect their sensitive medical information from quantum attacks by implementing additional security measures and closely monitoring their systems for any signs of unauthorized access or activity. Hence, certain scholars are focusing on developing novel cryptosystems that rely on quantum models and can be implemented on digital devices, not just quantum computers, and possess the adequate capability to withstand quantum attacks during the quantum age[8–10]. For example, Abd-El-Atty[11] developed a color image cipher approach using a logistic-sine map and quantum walks. This approach combines the probability distribution produced from quantum walk with the chaotic stream generated from the chaotic map using quaternions. In[5], Abd-El-Atty et al. developed a double medical image cipher algorithm using a logistic map and quantum walks. This approach splits two medical images into low and high 4-bit images, with the high 4-bit image being ciphered with quantum walks. Rehman et al.[12] proposed a new color image encryption scheme for medical images that combines quantum walks, Rubik's cube transformations, a hyperchaotic map, and the integration of elliptic curve cryptography with Hill Cipher. The scheme divides the plaintext image into a 3D cube, performs rotations and DNA encoding, and then combines the encoded cube with a chaotic cube through DNA addition. However, the DNA encoding and decoding operations are computationally intensive, especially for high-resolution images, making the scheme less efficient in terms of speed and performance, and the encryption scheme is vulnerable to plain image sensitivity attacks. The chaotic sequences produced by the chaotic systems in[5,8–12] do not rely on the running of quantum walks. Instead, these sequences are generated separately from the chaotic systems and quantum walks and then combined using quaternion[11], adapted particle swarm optimization[8,9], or summation processes[5,10].

Therefore, we need to develop a novel medical image cipher technique based on a quantum paradigm and a chaotic map in which the chaotic sequence produced from the chaotic mapping relies on the running of quantum walks and the pristine image, besides its initial conditions and control parameters.

Preliminaries

The cascading of quantum walks with the Chebyshev map is a novel approach that aims to capitalize on the strengths of both classical chaos theory and quantum mechanics in image encryption. In this section, we present the essential knowledge for designing the cascading system.

Chebyshev map

One of the most widely used one-dimensional chaotic mappings is Chebyshev map, which is represented as in Eq. (1).

$$x_i = \cos\left(\lambda \times \arccos(x_{i-1})\right) \tag{1}$$

with $x_i \in [-1, 1]$ is the initial condition of the chaotic mapping, and $\lambda \in N$ is the control parameter and $\lambda \geq 2$. For more illustrations about Chebyshev mapping, refer to[30,31].

Quantum walks

Quantum walks can be classified into two types: discrete-time and continuous-time. However, our focus in this work is solely on discrete-time quantum walk, as they are extensively utilized in the development of contemporary cryptographic systems[32]. To run a quantum walk with one particle on a circular path, two quantum systems are required: the walker space H_s and the coin particle $H_p \leftarrow \sin\sigma|1\rangle + \cos\ \sigma|0\rangle$, both of which exist in Hilbert space $H \leftarrow H_s \otimes H_p$. During each step of operating the quantum walk on a circular path, the binary string M controls whether the unitary transformation $\hat{R}_1$ or $\hat{R}_0$ is performed on the entire quantum system $|\psi\rangle$. If the j^{th} bit of M is 1, $\hat{R}_1$ is performed, otherwise, $\hat{R}_0$ is performed. If the j^{th} step is beyond the length of M, the transformation operator $\hat{R}_2$ is performed. The transformation operator $\hat{R}_0$ can be represented using Eq. (2).

$$\hat{R}_0 = \hat{S}(\hat{I} \otimes \hat{O}_0) \tag{2}$$

where $\hat{S}$ denotes the shift operator and can be expressed for acting quantum walk on a circular diagram with odd N-vertex as described in Eq. (3).

$$\hat{S} = \sum_{j}^{N} (|(j-1) \mod N, 0\rangle\langle j,1| + |(j+1) \mod N, 0\rangle\langle j,0|) \tag{3}$$

Also, the coin operator $\hat{O}_0$ can be defined in general as in Eq. (4)

$$\hat{O}_0 = \begin{pmatrix} \cos\theta_0 & \sin\theta_0 \\ \sin\theta_0 & -\cos\theta_0 \end{pmatrix} \tag{4}$$

Transformation operators $\hat{R}_1$ and $\hat{R}_2$ can be created in a similar manner as constructing $\hat{R}_0$, with $\theta_0, \theta_1, \theta_2 \in [0, \pi/2]$. The state of $|\psi\rangle_t$ after t steps can be expressed using Eq. (5).

$$|\psi\rangle_t = \left(\hat{R}_i\right)^t |\psi\rangle_0, i \in \{0, 1, 2\} \tag{5}$$

Quantum walks are the quantum counterparts of classical random walks, where a particle or quantum state over a graph evolves in superposition across all possible paths. Quantum walks exhibit unique properties, such as superposition, where particles can exist in multiple states simultaneously, and interference, where the paths can constructively or destructively interfere, affecting the probability of the particle's position. Measurements in quantum walks are performed at the end of the process to obtain information about the walker's position, and the final position yields a probability distribution reflecting the quantum walker's dynamics. It is expressed that the likelihood of finding the walker at location j following t steps is as follows.

$$Pd(j,t) = \left|\langle j,1| \left(\hat{R}_i\right)^t |\psi\rangle_0\right|^2 + \left|\langle j,0| \left(\hat{R}_i\right)^t |\psi\rangle_0\right|^2 \tag{6}$$

For more illustration, Fig. 1 provides examples of the quantum walk's probability distribution.

Proposed cipher mechanism

Medical images are crucial in healthcare as they allow clinicians to visualize internal structures and organs, detect lesions and abnormalities, and monitor disease progression and treatment outcomes. They also play a critical role in surgical planning and guidance, as well as the development and testing of new medical devices and treatments. However, the transmission and storage of medical images pose significant challenges due to the sensitive information they contain. Developing new and more effective medical image cipher algorithms is critical to ensuring the security and confidentiality of medical images and maintaining patient trust in the healthcare system. In this section, a new medical image cipher system based on cascading quantum walk with Chebyshev map is proposed. To fulfill a high sensitivity of the plain image for the presented cipher mechanism, the hashing algorithm SHA256 is executed on the plain medical image, and the resulting hash value is utilized to update initial parameters. By using these updated parameters, we act quantum walks to produce a probability distribution vector, which is then used along with the updated initial condition to iterate the cascading system and produce a chaotic sequence that relies on quantum walks and the pristine image. This sequence is utilized for the permutation process on the pristine image, as well as for ciphering the blocks of the confused image

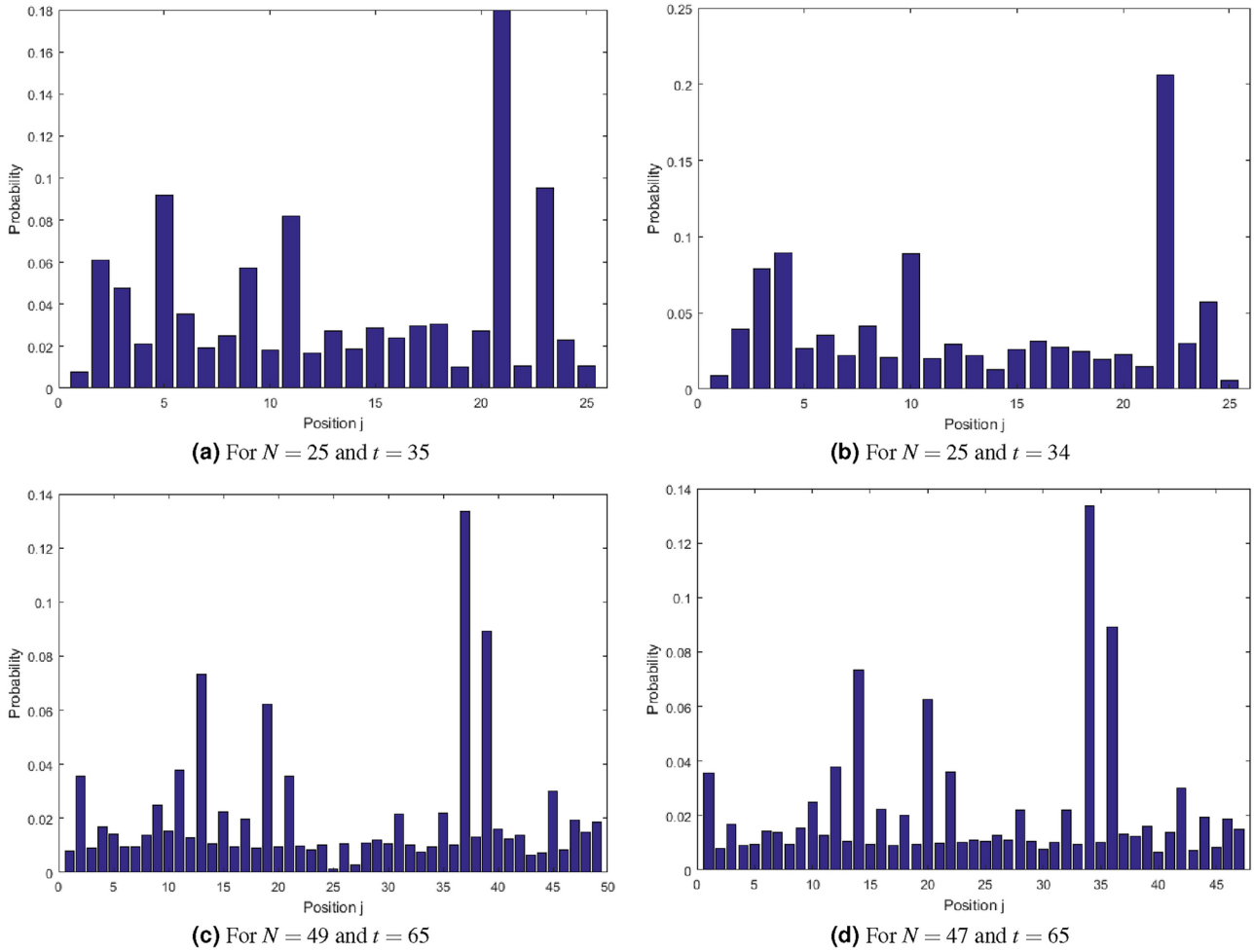


Figure 1. The probability distribution of running a quantum walk on a circular path of N vertices for t steps and controlled by the binary string "0100 1011 1011", in which the initial particle is $\sin \pi/6|1\rangle + \cos\ \pi/6|0\rangle$, $\theta_0 = \pi/6$, $\theta_1 = \pi/3$, and $\theta_2 = \pi/4$.

and performing the substitution process on the ciphered blocks. Figure 2 illustrates the block diagram of the presented cipher mechanism, and Algorithm 1 outlines the detailed steps involved in the cipher process. For more illustration, the detailed steps of the ciphering process are listed in the following points:

Input: Pristine medical image (PM)
Parameters : N, t, M, σ, θ_0, θ_1, θ_2, x_0, and λ
Output: Cipher-image (CM) and some information regarding the hash code ($d1$, $d2$)

$[P\ Q\ R] \leftarrow size(PM)$// Obtain the dimensions of the pristine medical image.
$H \leftarrow SHA256(PM)$// Compute the hash code for image PM.
$B \leftarrow uint8(H)$// Convert the hash code into 32 integers each of 8-bit.
$d1 \leftarrow (b_1 \oplus b_2 \oplus \cdots \oplus b_8)/256$
$d2 = \sum_{k=9}^{32} b_k$
// Updating the initial parameters M and x_0
$x_u \leftarrow (x_0 + d1)/2$
$M_u \leftarrow [M\ de2bi(d2)]$// Transform the integer value $d2$ to a binary structure then append it to M.
$Pd \leftarrow quantumWalk(N,t,M_u,\sigma,\theta_0,\theta_1,\theta_2)$// Act quantum walk on a circular diagram of odd N vertices for t steps and governed by M_u, in which the initial particle is $H_p \leftarrow \sin\sigma|1\rangle + \cos\sigma|0\rangle$, θ_0, θ_1, and θ_2 are used to construct the unitary transformations $\hat{R}_0$, $\hat{R}_1$, and $\hat{R}_2$, respectively, and $\sigma, \theta_0, \theta_1, \theta_2 \in [0, \pi/2]$.
$w \leftarrow resize(Pd, [1\ P \times Q \times R])$// Resize Pd of length N to w of length $P \times Q \times R$.
// Cascading system
$x_{i+1} \leftarrow \cos(\lambda \times \arccos((x_i + w_i)/2))$// Iterate the cascading system for $P \times Q \times R$ times, where the value of the initial condition x_0 is x_u.
$PMVec \leftarrow reshape(PM, P \times Q \times R, 1)$// Reshape the pixels of image PM to a one vector.
// Permutation process
$A \leftarrow sort(X)$// Arrange the items in sequence X in a way that they are sorted in increasing order.
$PVec \leftarrow index(X\ in\ A)$// Gather the index of each component in sequence X within sequence A.
for $k \leftarrow 1$ ***to*** $P \times Q \times R$ **do**
    $PerMVec(k) \leftarrow PMVec(PVec(k))$
// Constructing two permutation boxes each of length 32.
$C \leftarrow sort(X(1:32)$
$LP - box \leftarrow index(X(1:32)\ in\ C)$
$D \leftarrow sort(X(33:64)$
$RP - box \leftarrow index(X(33:64)\ in\ D)$
// Constructing two substitution boxes each consisting of 256 elements.
$E \leftarrow sort(X(65:320)$
$LS - box \leftarrow index(X(65:320)\ in\ E)$
$F \leftarrow sort(X(321:576)$
$RS - box \leftarrow index(X(321:576)\ in\ F)$
// Constructing a key sequence to perform the bitwise XOR process on the elements of each subblock.
$BKey \leftarrow \text{floor}(X \times 10^{12} \mod 256)$
$Blocks \leftarrow P \times Q \times R/64$// Obtain the count of image blocks, where each block comprises 64 pixels.
// Constructing a sequence to circular shift the elements of each subblock.
$CSB \leftarrow \text{floor}(X(1:2 \times Blocks) \times 10^8 \mod 32)$
$BS \leftarrow 1$// Initialization of subblock count

Algorithm 1. Ciphering algorithm

1. Choose initial values for key parameters (N, t, M, σ, θ_0, θ_1, θ_2, x_0, λ) to cipher the pristine medical image (PM) of dimensions $P \times Q \times R$.
2. Compute the hash code for image PM, and convert the hash code into 32 integers each of 8-bit to get two integers $d1$ and $d2$.

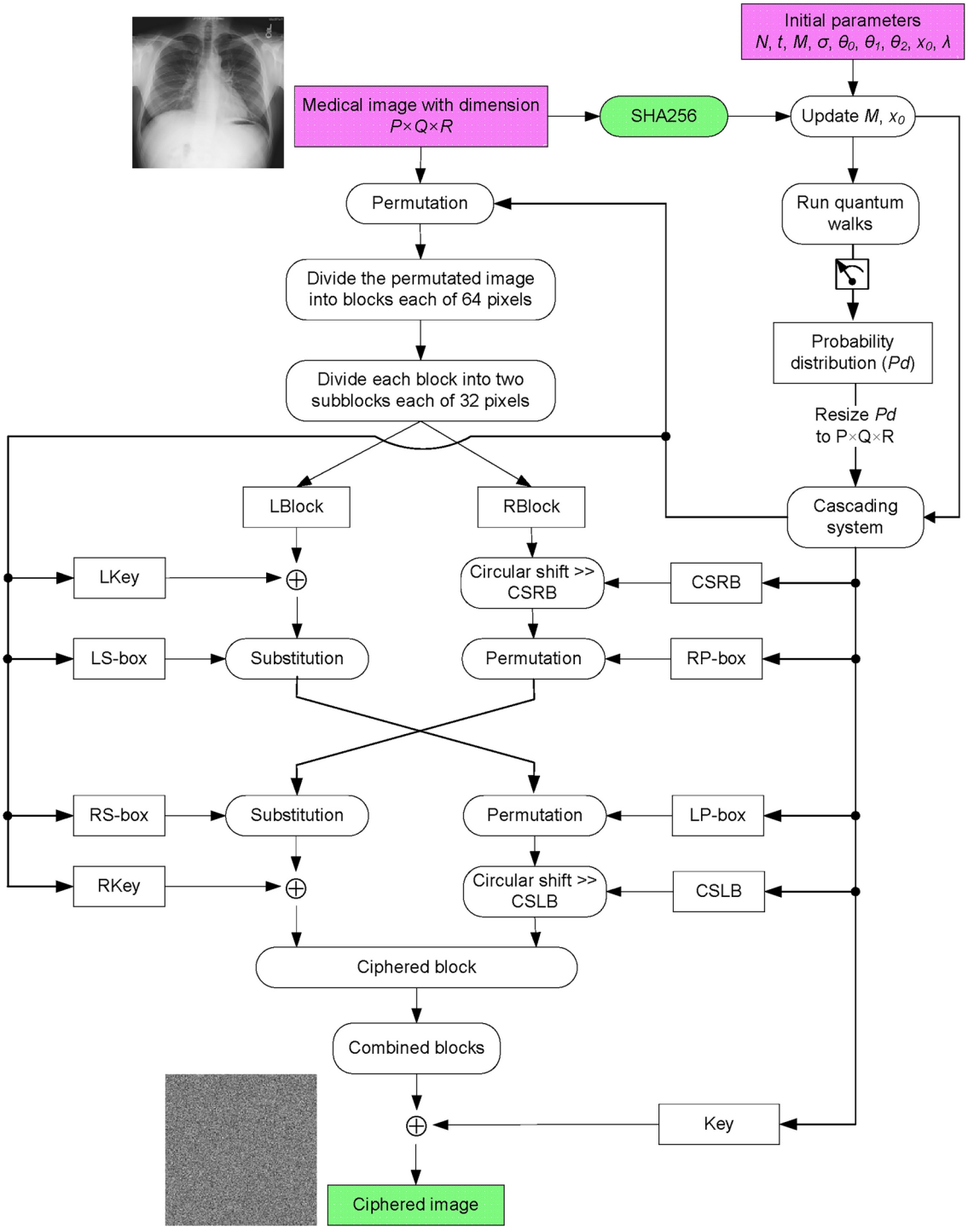


Figure 2. Block diagram of the presented cipher mechanism.

$$H = SHA256(PM) \tag{7}$$

$$B = uint8(H) \tag{8}$$

$$d1 = (b_1 \oplus b_2 \oplus \cdots \oplus b_8)/256 \tag{9}$$

$$d2 = \sum_{k=9}^{32} b_k \tag{10}$$

3. Update the initial control parameter x_0 of iterating the Chebyshev map using $d1$, and update the binary message M of controlling quantum walks by transforming the integer value $d2$ to a binary structure, then append it to the old value of M.

$$x_u = (x_0 + d1)/2 \tag{11}$$

$$M_u = [M \;\; de2bi(d2)] \tag{12}$$

4. Act quantum walk on a circular diagram of odd N vertices for t steps and governed by M_u for generating a probability distribution vector Pd of length N.

$$Pd = quantumWalk(N, t, M_u, \sigma, \theta_0, \theta_1, \theta_2) \tag{13}$$

in which the initial particle is $H_p \leftarrow \sin\sigma|1\rangle + \cos\ \sigma|0\rangle$, θ_0, θ_1, and θ_2 are used to construct the unitary transformations $\hat{R}_0$, $\hat{R}_1$, and $\hat{R}_2$, respectively, and $\sigma, \theta_0, \theta_1, \theta_2 \in [0, \pi/2]$.

5. Resize Pd of length N to w of length $P \times Q \times R$.

$$w = resize(Pd, [1 \;\; P \times Q \times R]) \tag{14}$$

6. Iterate the cascading system given in Eq. (15) for $P \times Q \times R$ times.

$$x_{i+1} = \cos(\lambda \times \arccos((x_i + w_i)/2)) \tag{15}$$

where the value of the initial condition x_0 is x_u. The main goal of the cascading system is to prevent the generation of periodic orbits in the resulting sequence. Measurements in quantum walks are carried out at the end of the process to obtain information about the walker's position, and the final position yields a probability distribution w reflecting the quantum walker's dynamics. Consequently, the value of w_{i+1} is not dependent on the value of w_i. Even if the value of x_i is repeated periodically, the value of w_i has a high probability of being different from its corresponding w_j value. Thus, the presented cascading system can avoid periodic orbits in the generated chaotic sequence.

7. Arrange the items in sequence X in a way that they are sorted in increasing order, and gather the index of each component in sequence X within sequence A as sequence $PVec$.

$$A = sort(X) \tag{16}$$

$$PVec = index(X \;\; in \;\; A) \tag{17}$$

8. Reshape the pixels of image PM to a vector $PMVec$, and permutate the pixels of the resulting vector $PMVec$ using $PVec$.

$$PMVec = reshape(PM, P \times Q \times R, 1) \tag{18}$$

$$PerMVec(k) = PMVec(PVec(k)), \quad for\ k = 1, 2, ..., P \times Q \times R \tag{19}$$

9. Divide the permutated image $PerMVec$ into blocks each of 64 pixels, and divide each block into two subblocks each of 32 pixels, then construct two permutation boxes from sequence X each of length 32 ($LP - box$ and $RP - box$) for permutating the subblocks.

$$C = sort(X(1:32) \tag{20}$$

$$LP - box = index(X(1:32) \ \ in \ \ C) \tag{21}$$

$$D = sort(X(33:64) \tag{22}$$

$$RP - box = index(X(33:64) \ \ in \ \ D) \tag{23}$$

10. Construct two substitution boxes from sequence X each consisting of 256 elements ($LS - box$ and $RS - box$) for substituting the subblocks.

$$E = sort(X(65:320) \tag{24}$$

$$LS - box = index(X(65:320) \ \ in \ \ E) \tag{25}$$

$$F = sort(X(321:576) \tag{26}$$

$$RS - box = index(X(321:576) \ \ in \ \ F) \tag{27}$$

11. Construct a key sequence *BKey* to perform the bitwise XOR process on the elements of each subblock.

$$BKey = \text{floor}(X \times 10^{12} \mod 256) \tag{28}$$

12. Perform the given steps in Algorithm 3 to perform the different permutation and substitution processes on each subblock and combine blocks.
13. After Combining the cipher blocks *CipherMBlocks*, construct a key sequence *Key* to perform the bitwise XOR process on the elements of *CipherMBlocks*, then reshape the result to construct the final cipher medical image *CM*.

$$Key = \text{floor}(X \times 10^{14} \mod 256) \tag{29}$$

$$CMVec = CipherMBlocks \oplus Key \tag{30}$$

$$CM = reshape(CMVec, P, Q, R) \tag{31}$$

$CipherMBlocks \leftarrow []$
for $k \leftarrow 1$ ***:64:*** $P \times Q \times R$ **do**
  $Block \leftarrow PerMVec(k : k+63)$
  $LBlock \leftarrow Block(1:32)$
  $RBlock \leftarrow Block(33:64)$
  $KeyBlock \leftarrow BKey(k : k+63)$
  $LKey \leftarrow KeyBlock(1:32)$
  $RKey \leftarrow KeyBlock(33:64)$
  $CSLB \leftarrow CSB(BS)$
  $CSRB \leftarrow CSB(BS+1)$
  // Operations on left subblock
  $SLBlock1 \leftarrow LBlock \oplus LKey$
  for $j \leftarrow 1$ ***to*** 32 **do**
    $SLBlock2(j) \leftarrow LS-box(SLBlock1(j)+1)-1$// Substitution process using $LS-box$.
  for $j \leftarrow 1$ ***to*** 32 **do**
    $PLBlock(j) \leftarrow SLBlock2(LP-box(j))$// Permutation process using $LP-box$.
  $CipherLBlock \leftarrow circshift(PLBlock>>CSLB)$// Circular right shift the elements of sequence $PLBlock$ by $CSLB$ positions.
  // Operations on right subblock
  $CSRBlock \leftarrow circshift(RBlock>>CSRB)$
  for $j \leftarrow 1$ ***to*** 32 **do**
    $PRBlock(j) \leftarrow CSRBlock(RP-box(j))$// Permutation process using $RP-box$.
  for $j \leftarrow 1$ ***to*** 32 **do**
    $SRBlock(j) \leftarrow RS-box(PRBlock(j)+1)-1$// Substitution process using $RS-box$.
  $CipherRBlock \leftarrow SRBlock \oplus RKey$
  $CipherMBlocks \leftarrow [CipherMBlocks; CipherRBlock; CipherLBlock]$// Combined ciphered blocks.
  $BS \leftarrow BS+2$
// Substituting the ciphered blocks
$Key \leftarrow \text{floor}(X \times 10^{14} \mod 256)$
$CMVec \leftarrow CipherMBlocks \oplus Key$
$CM \leftarrow reshape(CMVec, P, Q, R)$// Cipher medical image

Algorithm 2. Ciphering algorithm (continued).

$Blocks \leftarrow P \times Q \times R/64$// Obtain the count of image blocks, where each block comprises 64 pixels.
// Constructing a sequence to circular shift the elements of each subblock.
$CSB \leftarrow \text{floor}(X(1:2 \times Blocks) \times 10^8 \mod 32)$
$BS \leftarrow 1$// Initialization of subblock count
$CipherMBlocks \leftarrow []$
for $k \leftarrow 1$ ***:64:*** $P \times Q \times R$ **do**
  $Block \leftarrow PerMVec(k : k+63)$
  $LBlock \leftarrow Block(1:32)$
  $RBlock \leftarrow Block(33:64)$
  $KeyBlock \leftarrow BKey(k : k+63)$
  $LKey \leftarrow KeyBlock(1:32)$
  $RKey \leftarrow KeyBlock(33:64)$
  $CSLB \leftarrow CSB(BS)$
  $CSRB \leftarrow CSB(BS+1)$
  // Operations on left subblock
  $SLBlock1 \leftarrow LBlock \oplus LKey$
  for $j \leftarrow 1$ ***to*** 32 **do**
    $SLBlock2(j) \leftarrow LS-box(SLBlock1(j)+1)-1$// Substitution process using $LS-box$.
  for $j \leftarrow 1$ ***to*** 32 **do**
    $PLBlock(j) \leftarrow SLBlock2(LP-box(j))$// Permutation process using $LP-box$.
  $CipherLBlock \leftarrow circshift(PLBlock>>CSLB)$// Circular right shift the elements of sequence $PLBlock$ by $CSLB$ positions.
  // Operations on right subblock
  $CSRBlock \leftarrow circshift(RBlock>>CSRB)$
  for $j \leftarrow 1$ ***to*** 32 **do**
    $PRBlock(j) \leftarrow CSRBlock(RP-box(j))$// Permutation process using $RP-box$.
  for $j \leftarrow 1$ ***to*** 32 **do**
    $SRBlock(j) \leftarrow RS-box(PRBlock(j)+1)-1$// Substitution process using $RS-box$.
  $CipherRBlock \leftarrow SRBlock \oplus RKey$
  $CipherMBlocks \leftarrow [CipherMBlocks; CipherRBlock; CipherLBlock]$// Combined ciphered blocks.
  $BS \leftarrow BS+2$

Algorithm 3. Ciphering blocks.

Experimental results and analyses

To assess the presented method of ciphering images, we executed it on a PC powered by an Intel $Core^{TM}$ 2 Duo CPU 3 GHz and 4GB RAM, utilizing MATLAB software R2016b. The dataset employed comprised of ten medical images in greyscale of different sizes extracted from MedPix dataset[33] and labeled PMI01, PMI02, PMI03, PMI04, PMI05, PMI06, PMI07, PMI08, PMI09, and PMI10 (see Figures 3 and 4). The initial parameters for the image ciphering system were established as: N=261, t= 267, $\sigma=\pi/2$, $\theta_0=\pi/6$, $\theta_1=\pi/3$, $\theta_2=\pi/4$, x_0= 0.7585, λ=4, and M= [1100 1001 1011 0100 1110 0101 0101 0101 0001 0110 1111 0010 1010 1011 1001 0101 0010].

To assess the effectiveness of the proposed image cipher technique, it is necessary to evaluate its performance in terms of visual quality, the time required to cipher the medical image, and its ability to resist various types of security attacks, including randomness analysis, statistical analysis, differential attacks, key sensitivity, and occlusion attacks. The following subsections will explore these analyses to validate the effectiveness of the proposed cipher mechanism for medical images.

Visual quality

The visual quality of ciphered images refers to the extent to which a ciphered image preserves the visual details of the pristine image after encryption. The visual quality of the ciphered images is shown in Figs. 3 and 4 that are fully noised, in which the naked eye can't obtain useful information about the pristine image from the ciphered image. To quantitatively assess the quality of the ciphered images, two widely used metrics are applied: PSNR ("Peak Signal-to-Noise Ratio") and SSIM ("Structural Similarity Index Measure").

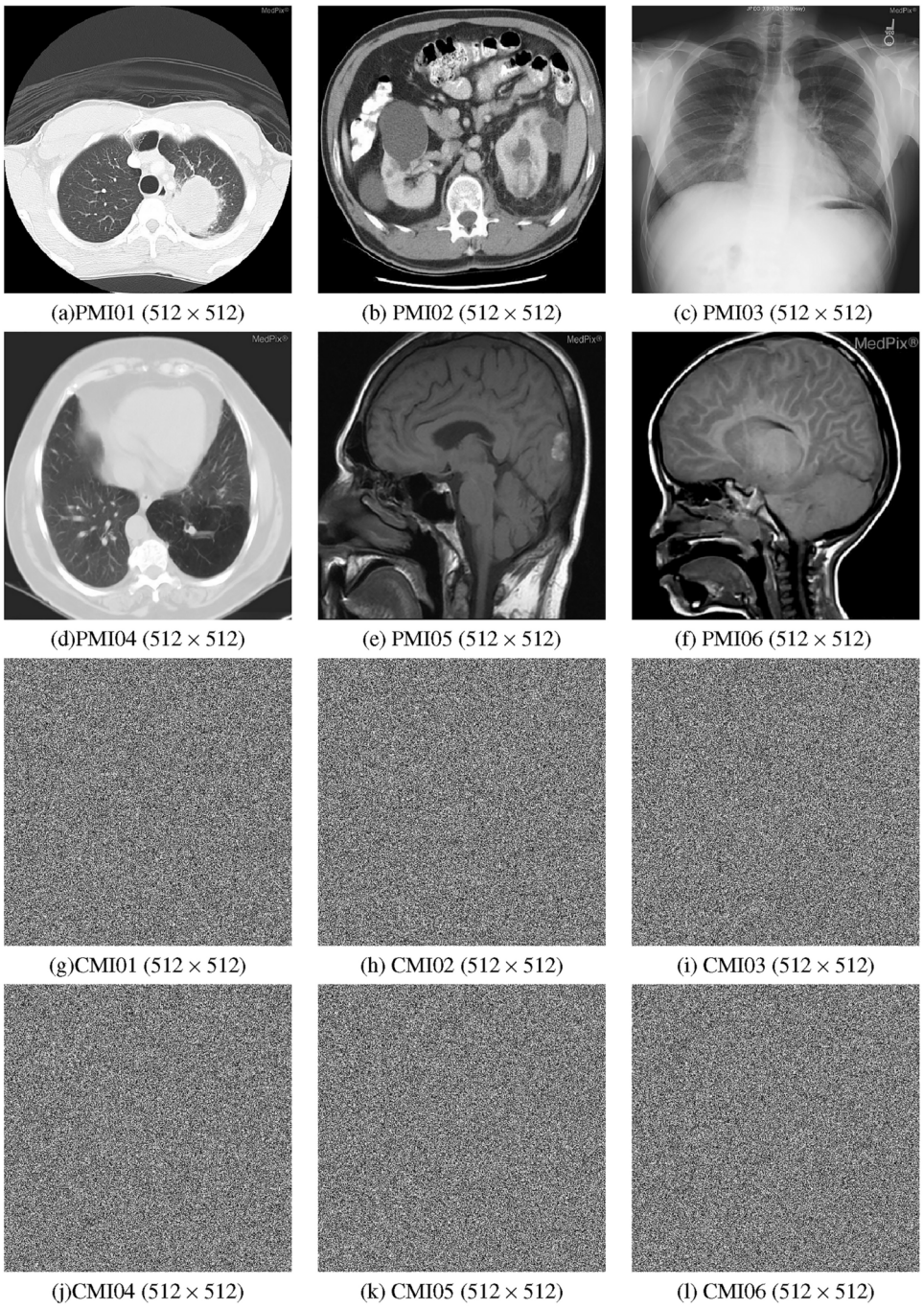


Figure 3. The collection of some examined images in which the top two rows depict the pristine images, and the bottom two rows display the ciphered versions of those images.

$$PSNR(PMI, CMI) = 10\log_{10}\left(\frac{MAX_{PMI} \times P \times Q}{\sum_{x=1}^{P}\sum_{y=0}^{Q}[PMI(x,y) - CMI(x,y)]^2}\right) \tag{32}$$

$$SSIM(PMI, CMI) = \frac{(C_1 + 2\mu_{PMI}\mu_{CMI})(C_2 + 2\sigma_{PMI,CMI})}{(C_1 + \mu_{PMI}^2 + \mu_{CMI}^2)(C_2 + \sigma_{PMI}^2 + \sigma_{CMI}^2)} \tag{33}$$

where the maximum pixel value of the pristine image *PMI* is MAX_{PMI}, and *CMI* represents its corresponding ciphered image, both of which have dimensions of $P \times Q$, and C_1, C_2 are constants, μ and σ refer to the mean and variance, respectively. PSNR quantifies the intensity difference between the ciphered and pristine images, where lower PSNR values signify that the ciphered image is highly distinct from the pristine. SSIM is another quality metric that assesses perceptual quality by focusing on structural similarity. It measures variations in

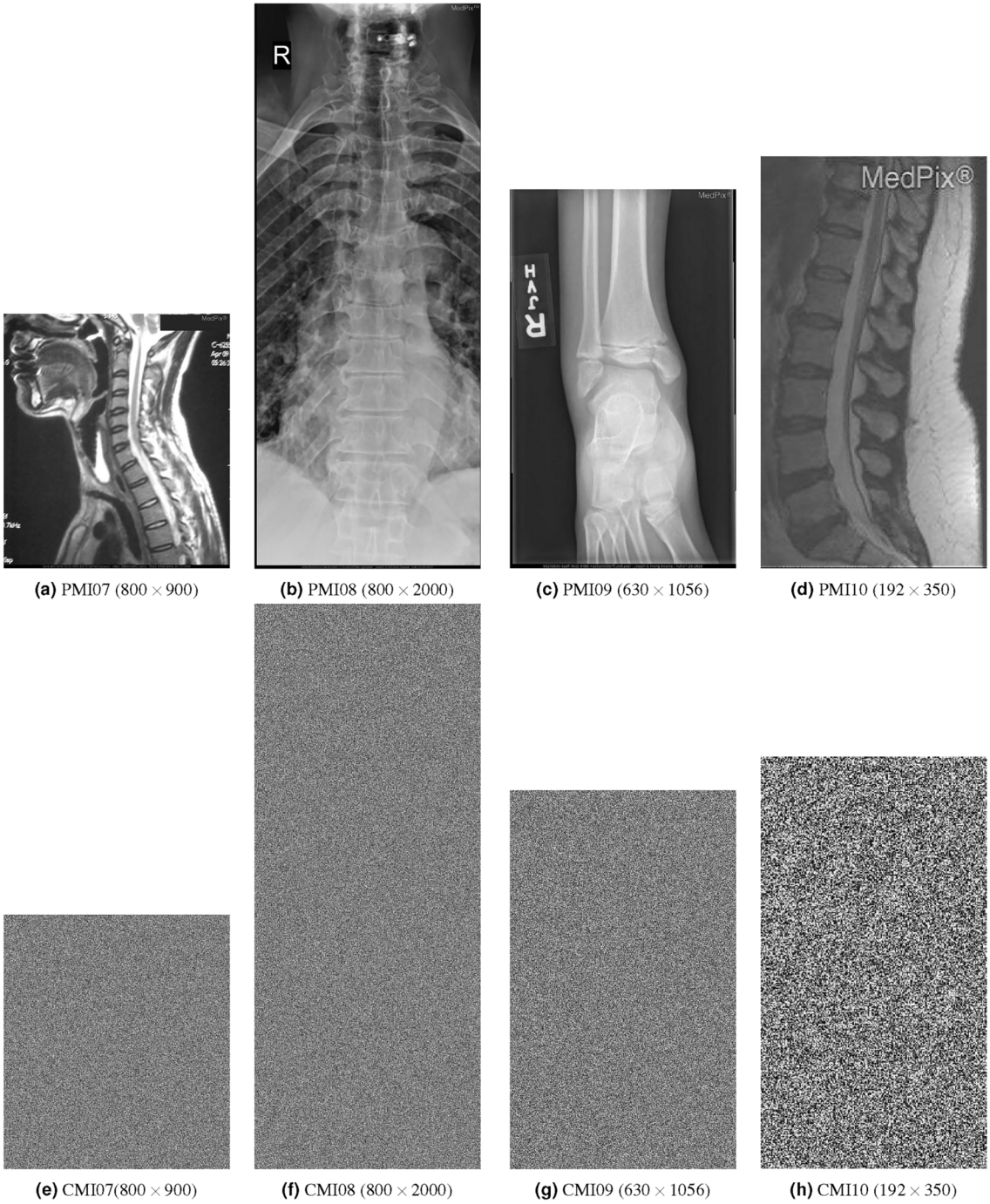


Figure 4. The collection of other examined images, in which the top row depicts the pristine images and the bottom row displays the ciphered versions of those images.

luminance, variance, and structure between two images, yielding a value from -1 to 1, with values closer to 1 indicating higher similarity. For ciphered images, a low SSIM value is typically desired, as it implies that the encryption has effectively obscured structural details. Table 1 presents the PSNR and SSIM values for ciphered images, where the low values indicate that the proposed cryptosystem generates secure cipher images with minimal visual quality resembling the original.

Ciphering-time efficiency

To evaluate the efficiency of the proposed cipher approach in terms of computational cost, we examine it from two perspectives: computational complexity and ciphering time.

Image	PSNR	SSIM
PMI01	6.5785	0.0293
PMI02	7.4147	0.0261
PMI03	8.1357	0.0382
PMI04	7.6730	0.0344
PMI05	7.5861	0.0277
PMI06	6.9632	0.0226
PMI07	7.9214	0.0516
PMI08	8.9210	0.0760
PMI09	7.9748	0.0346
PMI10	9.1317	0.0092

Table 1. PSNR and SSIM results.

Scheme	Image size			
	128×128	256×256	512×512	1024×1024
Proposed	0.05	0.24	2.96	12.36
Ref.[19]	1.74	6.87	28.76	113.75
Ref.[34]	3.27	15.26	-	-
Ref.[35]	-	2.44	-	-
Ref.[14]	-	4.83	-	-
Ref.[36]	-	5.35	-	-
Ref.[22]	-	-	1.53	-

Table 2. Comparison of ciphering times (in seconds) between our cipher system and other related systems for grayscale images of different sizes.

In terms of computational complexity, the encryption procedure comprises four main phases: key generation, confusion, block ciphering, and diffusion. The generated key sequence $\{X\}$ is produced using the proposed cascading system that based on the Chebyshev map and quantum walks. Running quantum walks on an N-vertex has a computational complexity of $\mathcal{O}(N^2)$, while the cascading system iterates $P \times Q$ times, where PQ represents the dimensions of the original image. Therefore, the computational complexity of the key generation phase is $\mathcal{O}(\max(N^2, PQ))$. The confusion phase is based on arranging the elements of sequence $\{X\}$ and determining the index of each element, with a complexity of $\mathcal{O}(PQ \log PQ)$. The block ciphering phase involves constructing two permutation boxes, two substitution boxes, and circular shifting of elements, each of which has a fixed computational complexity. The diffusion phase requires performing bitwise XOR operations with a complexity of $\mathcal{O}(8PQ)$. Combining the computational complexities of each phase, the total complexity of the proposed encryption scheme is $\mathcal{O}(\max(N^2, 8PQ, PQ \log PQ))$.

Regarding ciphering time, the time required to encrypt an image is a key criterion for evaluating the effectiveness of any image cipher system. To demonstrate the time efficiency of the proposed cipher system, Table 2 presents a straightforward comparison of ciphering times between our approach and other related methods. The results in Table 2 confirm that our method achieves an acceptable ciphering time.

Randomness analysis

In order to verify the randomness of the key produced from the cascading system and the constructed cipher images, we conducted NIST SP 800-22 tests, which include fifteen tests applied to a 10^6-bit sequence. Table 3 presents the results of these tests on the key stream (Key) used to cipher the pristine image PMI01 and the resulting cipher image CMI01, both of which passed all the randomness tests.

For more validation of the randomness of the generated sequences from the cascading system, we used the TestU01 suite, known for its comprehensive and rigorous testing capabilities. TestU01 offers several test batteries, including BigCrush, Crush, and SmallCrush. In this work, we used only the Crush (144 tests) and SmallCrush (15 tests) batteries due to the limited storage capacity of our PC. Also, we ran these tests with the default settings[37], making no modifications. The outcomes are stated in Table 4, showing that the cascading system sequences successfully passed all tests. The results presented in Tables 3 and 4 confirm the high level of randomness and unpredictability in the sequences generated by the cascading system, indicating that they can be reliably used in contemporary cryptographic systems.

Correlation analysis

Correlation coefficient (CC) of neighboring pixels is a widely used metric for assessing the meaningful of an image. In original images, CC values typically approach 1 in all directions, whereas in ciphered images with a good-designed cipher scheme, it should be close to 0. To assess CC in both the original and ciphered images,

Name of the test		P-Value		
		Key stream	CMI01	Passed
Linear complexity		0.185397	0.765490	✓
Overlapping templates		0.871481	0.343669	✓
Longest runs of ones		0.387833	0.873512	✓
Approximate entropy		0.098632	0.691866	✓
Runs		0.437367	0.568584	✓
Block-frequency		0.956940	0.878346	✓
DFT		0.890518	0.358795	✓
Universal statistical		0.569258	0.579931	✓
Frequency		0.421396	0.711382	✓
Rank		0.535630	0.702467	✓
Non-overlapping templates		0.818905	0.678795	✓
Random excursions	x=4	0.308777	0.260085	✓
Serial	Test 1	0.591346	0.791212	✓
	Test 2	0.923001	0.913817	✓
Cumulative sums	Forward	0.662438	0.887546	✓
	Reverse	0.537334	0.657794	✓
Random excursions variant	x=9	0.625987	0.010049	✓

Table 3. NIST SP 800-22 results.

Test battery	# Passed tests
Crush	144/144
SmallCrush	15/15

Table 4. TestU01 results.

we randomly chose 10^4 pairs of adjoining pixels per direction. The computation of *CC* can be carried out using Eq. (34).

$$CC = \frac{\sum_{k=1}^{R} (c_k - \bar{c})(p_k - \bar{p})}{\sqrt{\sum_{k=1}^{R} (c_k - \bar{c})^2 \sum_{k=1}^{R} (p_k - \bar{p})^2}} \tag{34}$$

with R representing the total number of pairs and c_k and p_k representing the values of the adjacent pixels. Table 5 presents the *CC* results for ciphered images and their corresponding pristine images, indicating that the ciphered image values are nearly zero. Additionally, Fig. 5 illustrates the correlation distribution per direction for the PMI01 image and its cipher counterpart. However, neither the *CC* values nor the correlation distribution provided any meaningful information about the ciphered image.

Differential analysis

Two tests, namely UACI ("Unified Average Changing Intensity") and NPCR ("Number of Pixels Change Rate"), are conducted to assess how sensitive the plain image is to even the slightest modifications. These tests can be expressed mathematically as follows:

$$\begin{aligned} NPCR &= \frac{\sum_{m;n} f(m,n)}{R} \times 100\%, \\ f(m,n) &= \begin{cases} 0 \; if \; CM1(m,n) = CM2(m,n) \\ 1 \; if \; CM1(m,n) \neq CM2(m,n) \end{cases} \end{aligned} \tag{35}$$

$$UACI = \frac{1}{R}\left(\sum_{m,n} \frac{|CM1(m,n) - CM2(m,n)|}{255}\right) \times 100\% \tag{36}$$

with the total number of pixels in the image is symbolized by R and $CM1$, $CM2$ are two ciphered images generated from a single pristine image, wherein a minor bit variation is introduced in one pixel. The findings of the UACI and NPCR tests are presented in Table 6, which confirm that even the slightest alterations in the pristine image can result in significant disparities in the resulting cipher image.

Image	H-D	V-D	D-D
PMI01	0.9861	0.9892	0.9798
CMI01	−0.0009	−0.0005	0.0001
PMI02	0.9795	0.9846	0.9670
CMI02	0.0008	−0.0012	−0.0005
PMI03	0.9943	0.9947	0.9920
CMI03	0.0005	−0.0008	0.0008
PMI04	0.9969	0.9950	0.9922
CMI04	−0.0007	−0.0005	−0.0004
PMI05	0.9899	0.9825	0.9695
CMI05	−0.0005	0.0007	−0.0008
PMI06	0.9846	0.9769	0.9607
CMI06	−0.0006	0.0002	−0.0001
PMI07	0.9870	0.9896	0.9787
CMI07	−0.0002	0.0002	0.0003
PMI08	0.9927	0.9926	0.9863
CMI08	−0.0001	−0.0002	0.0004
PMI09	0.9902	0.9869	0.9800
CMI09	0.0007	−0.0006	−0.0001
PMI10	0.9629	0.9682	0.9389
CMI10	−0.0005	−0.0001	0.0003

Table 5. *CC* results.

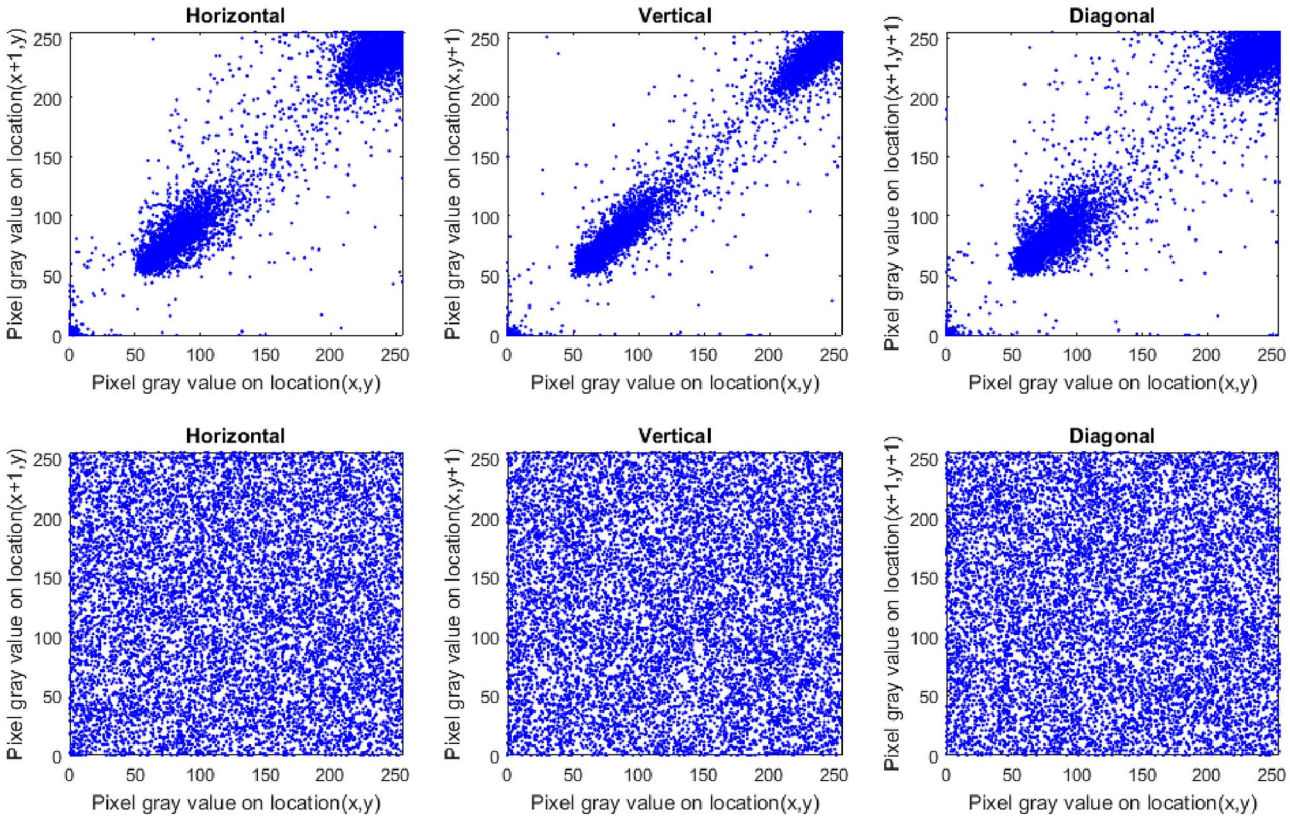


Figure 5. Distribution of correlation in each direction for the PMI01 image and its cipher counterpart, in which the foremost row shows the distribution for the PMI01 image while the bottommost row shows the distribution for the CMI01 image.

Image	UACI (%)	NPCR (%)
PMI01	33.4881	99.6398
PMI02	33.4626	99.6433
PMI03	33.4797	99.6246
PMI04	33.5056	99.6368
PMI05	33.4291	99.6326
PMI06	33.3974	99.6181
PMI07	33.4967	99.6135
PMI08	33.4754	99.6133
PMI09	33.4347	99.6187
PMI10	33.6402	99.6577

Table 6. Findings of the UACI and NPCR tests.

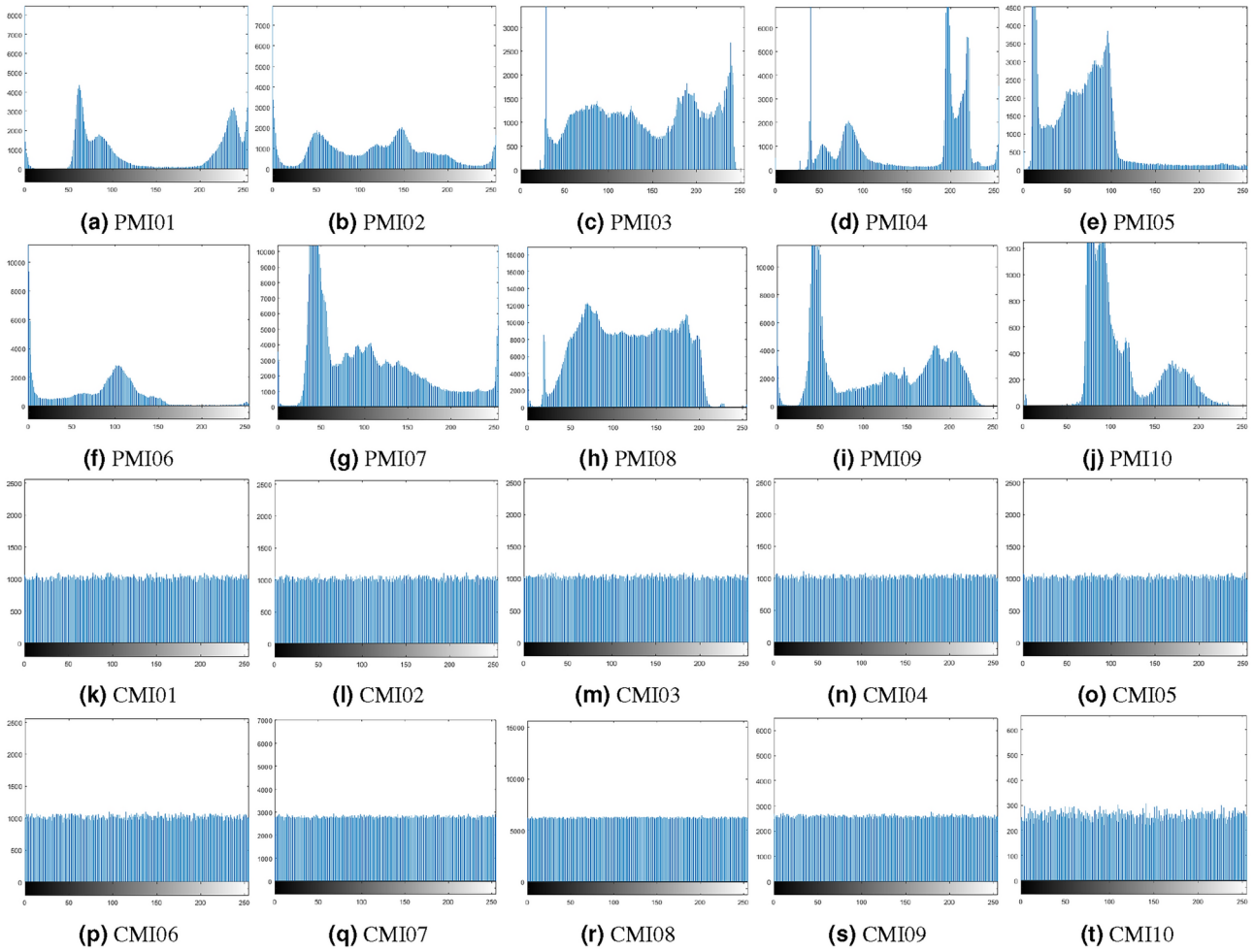


Figure 6. Histograms for plain and cipher images.

Histogram analysis

In order to demonstrate the distribution of pixels within an image, we employed the histogram tool, which requires that the histograms of various encrypted images be similar to one another, while the histograms of various pristine images should contrast from each other. Figure 6 depicts the histograms for plain and encrypted images, where the histograms of the ciphered images are indistinguishable from each other. However, as histogram is a subjective test, we also needed a quantitative test to assess the frequency of pixel distribution

within the image. For this purpose, we utilized the chi-square (χ^2) test, which can be expressed as shown in Eq. (37).

$$\chi^2 = \sum_{k=0}^{255} \frac{(y_k - z_k)^2}{z_k} \tag{37}$$

where the frequency of pixel k is denoted by y_k, and z_k represents the expected frequency under a uniform distribution. Assuming a significance level of 0.05, $\chi^2_{0.05}(255)$ is calculated to be 293.2478. If the χ^2 value for a given image is less than 293.2478, it indicates that the image has a uniform distribution of pixel frequencies. The χ^2 test results are presented in Table 7, where it can be observed that all cipher images have χ^2 values lower than 293.2478. Hence, the proposed cipher mechanism is capable of withstanding histogram attacks.

Entropy analysis

Global Shannon entropy is a statistical tool that assess the distribution of pixel values in an image, which can be calculated as follows:

$$E(X) = -\sum_{k=0}^{255} r(x_k) \log_2 (r(x_k)) \tag{38}$$

with $r(x_k)$ is the probability of x_k. For a greyscale image, there are 2^8 possible values, and the ideal entropy value is equivalent to 8-bit. To approve the efficacy of the proposed cipher system, the entropy value of the encrypted images should be close to 8. However, global entropy alone cannot determine the true randomness of ciphered images. Consequently, local entropy can be computed by calculating the mean of global entropies for non-overlapping blocks, each containing 1936 pixels. Table 8 shows the values of local and global entropies for both pristine and encrypted images, where all entropy values for encrypted images are very close to 8-bit. Thus, the proposed cipher system is secure against entropy analysis.

Keyspace and key sensitivity analyses

Keyspace refers to the range of possible keys available within a cryptosystem, essential for evaluating resilience against brute-force attacks. The proposed cryptosystem employs initial parameters (N, t, M, σ, θ_0, θ_1, θ_2, x_0, and λ) for operating quantum walks and iterating the cascading system. Although analyzing only the M parameter might suggest an infinite keyspace, the keyspace must be finite for practical implementation. Assuming the

Image	χ^2 value	Uniform
PMI01	2618949.5605	×
PMI02	2266799.5664	×
PMI03	211341.0585	×
PMI04	1635085.8261	×
PMI05	558187.1503	×
PMI06	4789957.1231	×
PMI07	861402.7967	×
PMI08	742878.0598	×
PMI09	1443567.6567	×
PMI10	175963.8324	×
CMI01	251.4082	✓
CMI02	256.7167	✓
CMI03	234.4003	✓
CMI04	217.1250	✓
CMI05	243.8750	✓
CMI06	266.3281	✓
CMI07	243.4801	✓
CMI08	228.8208	✓
CMI09	274.4034	✓
CMI10	272.6552	✓

Table 7. χ^2 test findings.

Image	Global entropy	Local entropy
PMI01	6.343323	4.994079
PMI02	6.969977	6.034518
PMI03	7.610096	5.498811
PMI04	6.462758	4.751234
PMI05	6.917889	5.645975
PMI06	6.110019	4.942486
PMI07	7.405730	5.660144
PMI08	7.540472	5.162985
PMI09	7.140514	4.527906
PMI10	6.645954	5.564518
CMI01	7.999309	7.902300
CMI02	7.999293	7.903337
CMI03	7.999355	7.903678
CMI04	7.999402	7.901939
CMI05	7.999327	7.902290
CMI06	7.999266	7.903201
CMI07	7.999756	7.901813
CMI08	7.999897	7.902105
CMI09	7.999703	7.902022
CMI10	7.997074	7.902422

Table 8. Outcomes of global and local entropies.

computational precision of digital devices is 10^{-16}, the keyspace of the proposed cryptosystem is 10^{144}, which is sufficiently large for use in modern cryptosystems.

Key sensitivity ensures that even slight modifications in the encryption key result in a significantly different encrypted image. In order to assess the key sensitivity of the mechanism being presented, slight variations in the ciphered keys were used to decipher the CMI01 image, as depicted in Fig. 7. To quantitatively assess key sensitivity, we employed the NPCR test, with results provided in Table 9. Based on the outcomes in Fig. 7 and Table 9, the proposed cryptosystem demonstrates a high sensitivity to small variations in key parameters.

Noise and data loss attacks analyses

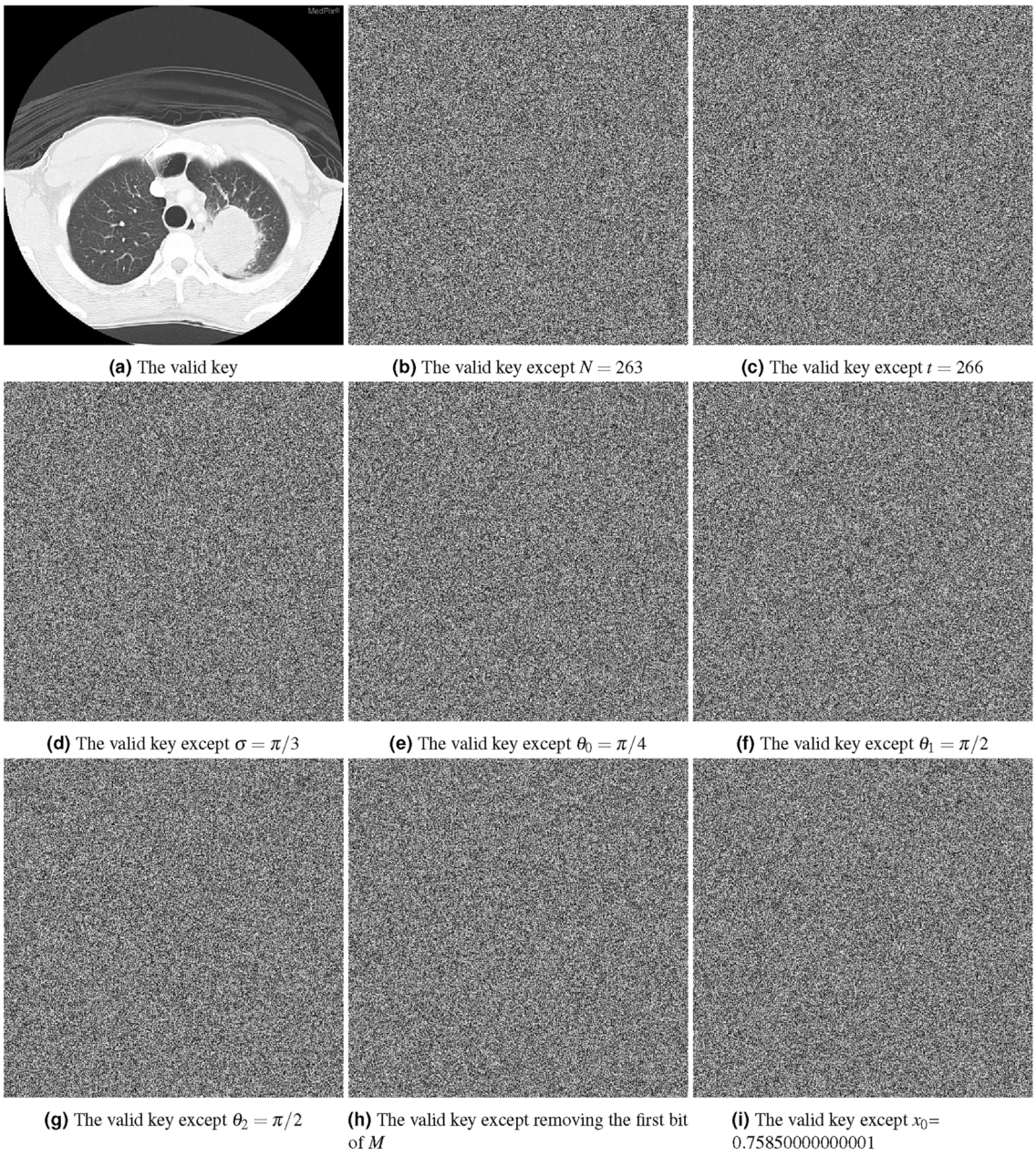
Noise and data loss attacks can occur during data transmission over communication channels, such as a network or the Internet. These attacks can introduce noise or lead to the loss of portions of the transmitted data, potentially compromising its integrity and security. To mitigate such risks, encryption algorithms should be designed to be robust, capable of withstanding occlusion attacks and enabling data recovery without loss of information. In the context of the proposed cryptosystem, the effectiveness of the cipher technique against these attacks was tested by removing portions of the cipher image or adding Salt & Pepper noise, then attempting to recover the original image from the flawed ciphered image. The results, shown in Figs. 8 and 9, demonstrate that the cryptosystem successfully retrieved the original image without any loss of information in the modified sections.

Discussion

This paper presented a new medical image cipher mechanism based on cascading quantum walk with Chebyshev map, which the main goal of the cascading system is to prevent the generation of periodic orbits in the resulting sequence. To fulfill a high sensitivity of the plain image for the presented cipher mechanism, the hashing algorithm SHA256 is executed on the plain medical image, and the resulting hash value is utilized to update initial parameters. By using these updated parameters, we act quantum walks to produce a probability distribution vector, which is then used along with the updated initial condition to iterate the Chebyshev map and produce a chaotic sequence that relies on quantum walks and the pristine image. This sequence is used for the confusion phase of the pristine image, as well as for ciphering the blocks of the confused image and performing the diffusion phase for the ciphered blocks. Our simulation outcomes and numerical analyses have demonstrated that this cipher mechanism is both secure and highly efficient.

To evaluate the effectiveness of the proposed image encryption technique, its performance is assessed in terms of visual quality, computational cost, and resilience to various types of security attacks, including randomness analysis, statistical analysis, differential attacks, key sensitivity, and occlusion attacks. In what follows, will explore the results of these analyses to validate the effectiveness of the proposed cipher mechanism for medical images.

From the perspective of visual quality, which refers to the extent to which a ciphered image preserves the visual details of the pristine image after encryption, The visual quality of the ciphered images was shown in Figs. 3 and 4 that are fully noised, and the naked eye can't obtain useful information about the pristine image from the ciphered image. To quantitatively assess the quality of the ciphered images, two metrics were applied: PSNR and SSIM. Table 1 presented the PSNR and SSIM values for ciphered images, where the low values indicate that the proposed cryptosystem generates secure cipher images with minimal visual quality.



(a) The valid key **(b)** The valid key except $N = 263$ **(c)** The valid key except $t = 266$

(d) The valid key except $\sigma = \pi/3$ **(e)** The valid key except $\theta_0 = \pi/4$ **(f)** The valid key except $\theta_1 = \pi/2$

(g) The valid key except $\theta_2 = \pi/2$ **(h)** The valid key except removing the first bit of M **(i)** The valid key except x_0= 0.75850000000001

Figure 7. Visual effects of key sensitivity.

Image	NPCR (%)
Figure 7a, b	99.6124
Figure 7a, c	99.6296
Figure 7a, d	99.6185
Figure 7a, e	99.6281
Figure 7a, f	99.6132
Figure 7a, g	99.6254
Figure 7a, h	99.6147
Figure 7a, i	99.6124

Table 9. Quantitative results of key sensitivity.

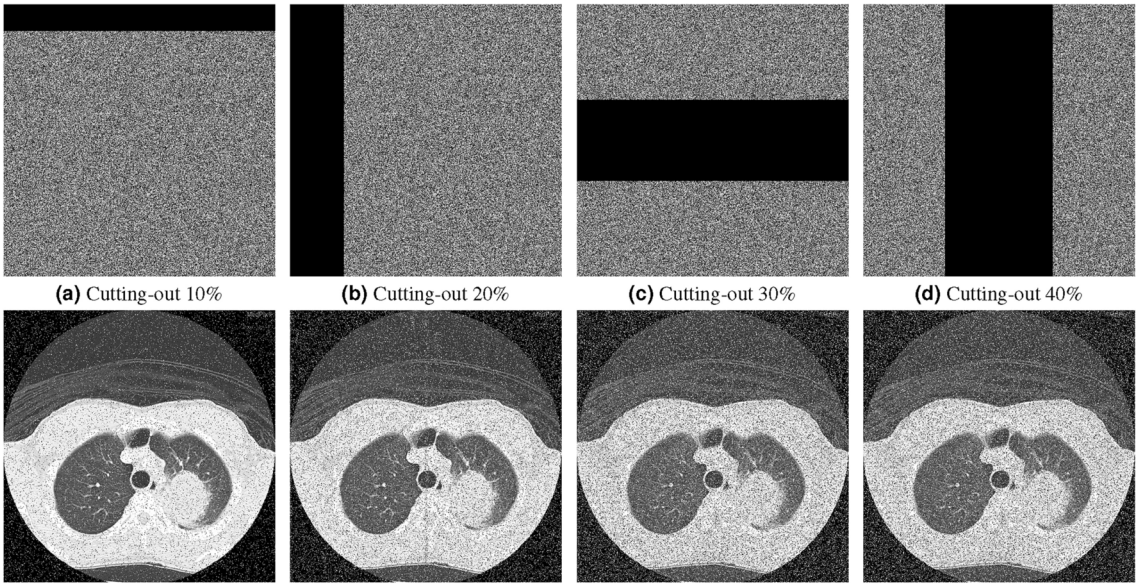


Figure 8. Effects of data loss attacks, in which the highest row shows the flawed ciphered images resulting from the removal of some of their slices, while the bottom row depicts the corresponding deciphered images.

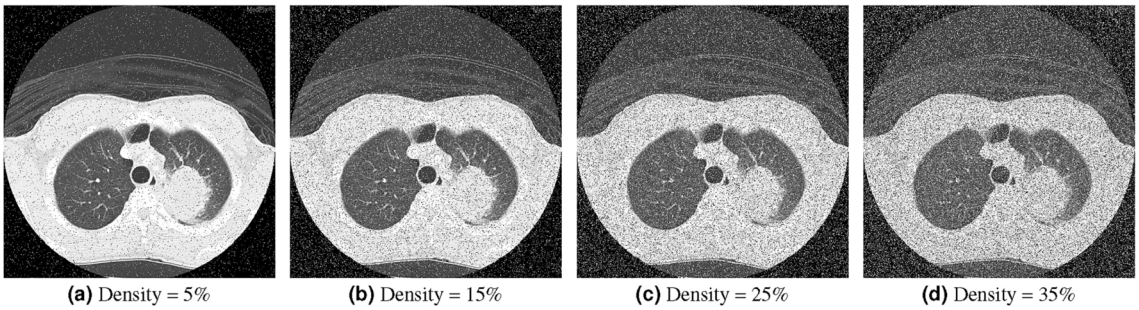


Figure 9. Effects of noise attacks with different Salt & Pepper noise densities, where the images shown are the deciphered results of the flawed ciphered images at each specified Salt & Pepper noise density.

From the perspective of computational cost, the presented cryptosystem was evaluated from two viewpoints: computational complexity and ciphering time. The computational complexity of the proposed encryption scheme is $\mathcal{O}(\max(N^2, 8PQ, PQ\log PQ))$, which is acceptable for modern cryptosystems. To demonstrate the time efficiency of the proposed cipher system, Table 2 presented a straightforward comparison of ciphering times between our approach and other related methods. The computational cost results confirm that our method achieves a satisfactory ciphering time plus acceptable computational complexity.

Regarding resilience to various types of security attacks, several analyses were conducted, including randomness analysis, statistical analysis, differential attacks, key sensitivity, and occlusion attacks. To verify the randomness of the key generated by the cascading system, Table 3 presents the results of NIST SP 800-22 tests on the keystream used to encrypt the original image PMI01 and the resulting ciphered image CMI01, both of which passed all randomness tests. For further validation of the randomness of the sequences generated by the cascading system, we used the TestU01 suite, with results shown in Table 4, indicating that the cascading system sequences successfully passed all tests. The results presented in Tables 3 and 4 confirm the high level of randomness and unpredictability in the sequences generated by the cascading system, demonstrating that they can be reliably used in contemporary cryptographic systems. The correlation coefficient of neighboring pixels is a widely used statistical metric for assessing the structure of an image. In original images, *CC* values typically approach 1 in all directions, whereas in ciphered images with a well-designed cipher scheme, it should be close to 0. Table 5 presented the *CC* results for ciphered images and their corresponding pristine images. The average values of *CC* per direction are -0.00015, -0.00028, 0.00000, indicating that the ciphered image values are nearly zero. Additionally, Fig. 5 illustrates the correlation distribution per direction for the PMI01 image and its cipher counterpart. However, neither the *CC* values nor the correlation distribution reveal any meaningful information about the ciphered image. To assess the sensitivity of the plain image to minor modifications, two differential tests were used: UACI and NPCR. Table 6 provides the outcomes of these tests. The average values of UACI and NPCR are 33.48095% and 99.62984%, respectively, confirming that even the slightest alterations

Algorithm	UACI %	NPCR %	χ^2	Information entropy		Correlation		
				Local	Global	H-D	V-D	D-D
Proposed	33.48095	99.62984	248.92128	7.90279	7.99923	-0.00015	-0.00028	0.00000
Ref.[5]	33.46590	99.61420	252.65270	7.90251	7.99924	-0.00010	0.00020	-0.00010
Ref.[11]	33.45969	99.61070	255.90407	7.90254	7.99984	0.00003	-0.00004	-0.00008
Ref.[9]	33.48400	99.61800	249.48100	-	7.99977	0.00015	-0.00031	-0.00004
Ref.[36]	33.44000	99.60000	257.33700	-	7.99700	-0.00970	-0.00870	0.00650
Ref.[20]	33.65836	99.60876	–	7.61791	7.75345	0.00220	0.00200	0.00230
Ref.[14]	32.05333	99.60667	–	-	7.99721	0.01360	0.00978	-0.00333
Ref.[15]	33.46700	99.62900	–	-	7.99752	0.00154	-0.00310	0.00090
Ref.[16]	33.45941	99.60012	–	-	7.99786	0.00382	-0.00425	0.00251
Ref.[17]	33.50000	99.61000	–	-	7.99818	-0.00160	0.00430	- 0.00610
Ref.[21]	33.45960	99.60090	–	-	7.99980	0.00270	0.00310	0.00110
Ref.[22]	33.50888	99.61333	–	-	7.99907	0.00041	0.00161	-0.00011
Ref.[19]	33.56650	99.60850	–	-	7.99660	-	-	-

Table 10. Comparative analysis of the presented cipher technique against other related cipher systems.

in the pristine image can lead to significant differences in the resulting ciphered image. To illustrate the pixel distribution within an image, we used the histogram tool. Figure 6 showed the histograms for both the plain and ciphered images, where the histograms of the ciphered images appear indistinguishable from each other. However, since the histogram is a visual test, we also employed the χ^2 test. Table 7 provides the χ^2 test results, showing that all encrypted images have χ^2 values lower than 293.2478, indicating a uniform distribution of pixel frequencies in the encrypted images. Thus, the proposed encryption mechanism is capable of withstanding histogram attacks. To assess the randomness of pixel values within encrypted images, we utilized local and global entropy measurements. Table 8 presents the local and global entropy values for both the original and encrypted images, showing that all entropy values for the encrypted images are very close to the maximum 8-bit value. This indicates that the proposed encryption system is secure against entropy analysis. Keyspace and key sensitivity are essential metrics to evaluate the security of any image cryptosystem. The keyspace of the proposed cryptosystem is 10^{144}, which is sufficiently large for use in modern cryptosystems. For assessing the key sensitivity, slight variations in the ciphered keys were used to decipher the CMI01 image, as depicted in Fig. 7. To quantitatively assess key sensitivity, we employed the NPCR test, with results provided in Table 9. Based on the outcomes in Fig. 7 and Table 9, the proposed cryptosystem demonstrates a high sensitivity to small variations in key parameters. To assess the effectiveness of the proposed cryptosystem against occlusion attacks, portions of the ciphered image were removed at various sizes, or Salt & Pepper noise was added at different densities, and then an attempt was made to recover the original image from the altered ciphered image. The results, shown in Figs. 8 and 9, demonstrate that the cryptosystem successfully retrieved the original image without any information loss in the modified sections.

When evaluating the effectiveness of an encryption mechanism, it is important to compare its performance against other similar cryptosystems. This permits us to decide if the proposed system is indeed an improvement over existing systems and whether it provides adequate security for the intended application. Table 10 provides a comparative analysis of the presented cipher mechanism against other related cipher systems. It presents the average values of several metrics, including Chi-square, UACI, NPCR, information entropy, and correlation, which are commonly utilized to estimate the effectiveness of cipher algorithms. By comparing the average values of these metrics for the presented cipher algorithm with those of other related cryptosystems, the efficacy of the proposed system can be inferred.

Conclusion and futur works

The primary objective of this study is to open the way for the development of modern cipher systems that can withstand quantum attacks during the quantum age by using cascading quantum models with chaotic maps. This paper has proposed a new medical image cipher algorithm using cascading quantum walk with the Chebyshev map, which its experimental results have been analyzed and demonstrated high levels of security and efficiency. The main limitations of the proposed cryptosystem are: (1) it is restricted to encrypting medical images of specific sizes, where the product of the image dimensions must be divisible by 64 due to the cipher block phase; and (2) it is tailored exclusively for image data and is unsuitable for other data types. In future work, our objective is to investigate practical implementation challenges and scalability in real-world scenarios, such as IoT and 5G/6G networks, through extensive experimentation and performance evaluation. We also plan to address the current limitations and explore enhancements, including integration with post-quantum cryptographic techniques, to improve the system's robustness and applicability.

Data availability

The data used in the study are openly available in the public at https://medpix.nlm.nih.gov/home reference number[33].

Code availability

This paper outlines the algorithmic steps and provides a detailed analysis. For access to the code or research materials, please contact the corresponding author, with necessary agreements in place to protect intellectual property.

Received: 4 May 2024; Accepted: 14 February 2025
Published online: 25 February 2025

References

1. Santhi, k. A survey on medical imaging techniques and applications. *J. Innov. Image Process.* **4**, 173–182. https://doi.org/10.36548/jiip.2022.3.005 (2022).
2. Zhang, Y. & Dong, Z. Medical imaging and image processing. *Technologies* **11**, 54. https://doi.org/10.3390/technologies11020054 (2023).
3. Panayides, A. S. et al. AI in medical imaging informatics: Current challenges and future directions. *IEEE J. Biomed. Health Inform.* **24**, 1837–1857. https://doi.org/10.1109/jbhi.2020.2991043 (2020).
4. Gadde, S., Amutharaj, J. & Usha, S. A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *J. Inf. Secur. Appl.* **73**, 103412. https://doi.org/10.1016/j.jisa.2022.103412 (2023).
5. Abd-El-Atty, B., Elaffendi, M., Chelloug, S. A. & El-Latif, A. A. A. Double medical image cryptosystem based on quantum walk. *IEEE Access*. 1–12. https://doi.org/10.1109/access.2023.3289932 (2023).
6. Tang, Z., Chai, X., Lu, Y., Wang, B. & Tan, Y. An end-to-end screen shooting resilient blind watermarking scheme for medical images. *J. Inf. Secur. Appl.* **76**, 103547. https://doi.org/10.1016/j.jisa.2023.103547 (2023).
7. Abd-El-Atty, B. A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. *Neural Comput. Appl.* **35**, 773–785. https://doi.org/10.1007/s00521-022-07830-0 (2022).
8. Abd-El-Atty, B. & EL-Latif, A. A. A. Applicable image cryptosystem using bit-level permutation, particle swarm optimisation, and quantum walks. *Neural Comput. Appl.*[SPACE]https://doi.org/10.1007/s00521-023-08643-5 (2023).
9. Abd-El-Atty, B. Efficient s-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem. *Complex Intell. Syst.*[SPACE]https://doi.org/10.1007/s40747-023-00988-7 (2023).
10. Abd-El-Atty, B., ElAffendi, M. & El-Latif, A. A. A. A novel image cryptosystem using gray code, quantum walks, and henon map for cloud applications. *Complex Intell. Syst.* **9**, 609–624. https://doi.org/10.1007/s40747-022-00829-z (2023).
11. Abd-El-Atty, B. Quaternion with quantum walks for designing a novel color image cryptosystem. *J. Inf. Secur. Appl.* **71**, 103367. https://doi.org/10.1016/j.jisa.2022.103367 (2022).
12. Rehman, M. U., Shafique, A. & Usman, A. B. Securing medical information transmission between IOT devices: An innovative hybrid encryption scheme based on quantum walk, DNA encoding, and chaos. *Internet Things* **24**, 100891. https://doi.org/10.1016/j.iot.2023.100891 (2023).
13. Niu, Y., Zhou, H. & Zhang, X. Image encryption scheme based on improved four-dimensional chaotic system and evolutionary operators. *Sci. Rep.* **14**, 7033. https://doi.org/10.1038/s41598-024-57756-x (2024).
14. El-Shafai, W., Khallaf, F., El-Rabaie, E.-S.M. & El-Samie, F. E. A. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *J. Ambient Intell. Hum. Comput.* **12**, 9007–9035. https://doi.org/10.1007/s12652-020-02597-5 (2021).
15. Abdelfatah, R. I., Saqr, H. M. & Nasr, M. E. An efficient medical image encryption scheme for (WBAN) based on adaptive DNA and modern multi chaotic map. *Multimed. Tools Appl.* **82**, 22213–22227. https://doi.org/10.1007/s11042-022-13343-8 (2022).
16. Guesmi, R. & Farah, M. A. B. A new efficient medical image cipher based on hybrid chaotic map and DNA code. *Multimed. Tools Appl.* **80**, 1925–1944. https://doi.org/10.1007/s11042-020-09672-1 (2020).
17. Dagadu, J. C., Li, J.-P. & Aboagye, E. O. Medical image encryption based on hybrid chaotic DNA diffusion. *Wirel. Pers. Commun.* **108**, 591–612. https://doi.org/10.1007/s11277-019-06420-z (2019).
18. Liu, H., Teng, L., Zhang, Y., Si, R. & Liu, P. Mutil-medical image encryption by a new spatiotemporal chaos model and DNA new computing for information security. *Expert Syst. Appl.* **235**, 121090. https://doi.org/10.1016/j.eswa.2023.121090 (2024).
19. Jain, K., Aji, A. & Krishnan, P. Medical image encryption scheme using multiple chaotic maps. *Pattern Recognit. Lett.* **152**, 356–364. https://doi.org/10.1016/j.patrec.2021.10.033 (2021).
20. Belazi, A. et al. Improved sine-tangent chaotic map with application in medical images encryption. *J. Inf. Secur. Appl.* **66**, 103131. https://doi.org/10.1016/j.jisa.2022.103131 (2022).
21. Lai, Q., Hu, G., Erkan, U. & Toktas, A. High-efficiency medical image encryption method based on 2d logistic-gaussian hyperchaotic map. *Appl. Math. Comput.* **442**, 127738. https://doi.org/10.1016/j.amc.2022.127738 (2023).
22. Masood, F. et al. A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wirel. Pers. Commun.* **127**, 1405–1432. https://doi.org/10.1007/s11277-021-08584-z (2021).
23. Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M. & Fouda, M. M. A new image encryption algorithm for grey and color medical images. *IEEE Access* **9**, 37855–37865. https://doi.org/10.1109/access.2021.3063237 (2021).
24. Zhuang, Z., Zhuang, Z. & Wang, T. Medical image encryption algorithm based on a new five-dimensional multi-band multi-wing chaotic system and QR decomposition. *Sci. Rep.* **14**, 402. https://doi.org/10.1038/s41598-023-50661-9 (2024).
25. Zhang, Z., Tang, J., Zhang, F., Huang, T. & Lu, M. Medical image encryption based on josephus scrambling and dynamic cross-diffusion for patient privacy security. In *IEEE Transactions on Circuits and Systems for Video Technology*. 1–1. https://doi.org/10.1109/tcsvt.2024.3394951 (2024).
26. El-Latif, A. A. A., Abd-El-Atty, B. & Talha, M. Robust encryption of quantum medical images. *IEEE Access* **6**, 1073–1081. https://doi.org/10.1109/access.2017.2777869 (2018).
27. Aparna, H. et al. Double layered Fridrich structure to conserve medical data privacy using quantum cryptosystem. *J. Inf. Secur. Appl.* **63**, 102972. https://doi.org/10.1016/j.jisa.2021.102972 (2021).
28. Prajapat, S., Kumar, D. & Kumar, P. Quantum image encryption protocol for secure communication in healthcare networks. *Cluster Comput.* **28**. https://doi.org/10.1007/s10586-024-04743-6 (2025).
29. Kadhim, A. J. & Atia, T. S. Quantum encryption of healthcare images: Enhancing security and confidentiality in e-health systems. *Secur. Privacy* **7**. https://doi.org/10.1002/spy2.391 (2024).
30. Rosen, J., Scherr, Z., Weiss, B. & Zieve, M. E. Chebyshev mappings of finite fields. *Am. Math. Mon.* **119**, 151. https://doi.org/10.4169/amer.math.monthly.119.02.151 (2012).
31. Kohda, T., Tsuneda, A. & Lawrance, A. J. Correlational properties of Chebyshev chaotic sequences. *J. Time Ser. Anal.* **21**, 181–191. https://doi.org/10.1111/1467-9892.00180 (2000).
32. Venegas-Andraca, S. E. Quantum walks: A comprehensive review. *Quantum Inf. Process.* **11**, 1015–1106. https://doi.org/10.1007/s11128-012-0432-5 (2012).
33. The National Library of Medicine. https://medpix.nlm.nih.gov/home. Accessed 1 July 2023.
34. Saravanan, S. & Sivabalakrishnan, M. A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. *Soft Comput.* **25**, 5299–5322. https://doi.org/10.1007/s00500-020-05528-w (2021).

35. Farah, M. A. B., Farah, A. & Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn.* **99**, 3041–3064. https://doi.org/10.1007/s11071-019-05413-8 (2019).
36. hua Gan, Z., li Chai, X., jun Han, D. & ran Chen, Y. A chaotic image encryption algorithm based on 3-d bit-plane permutation. *Neural Comput. Appl.* **31**, 7111–7130. https://doi.org/10.1007/s00521-018-3541-y (2018).
37. LEcuyer, P. & Simard, R. Testu01: A c library for empirical testing of random number generators. *ACM Trans. Math. Softw.* **33**, 1–40. https://doi.org/10.1145/1268776.1268777 (2007).

Acknowledgements
This work was funded by the Researchers Supporting Project No. (RSPD2025R564), King Saud University, Riyadh, Saudi Arabia.

Author contributions
These authors contributed equally to this research.

Funding
This work was funded by the Researchers Supporting Project No. (RSPD2025R564), King Saud University, Riyadh, Saudi Arabia.

Declarations

Competing interests
The authors declare no competing interests.

Ethics and methods approval
We confirm that all methods were carried out in accordance with relevant guidelines and regulations. In addition, all experimental/simulation protocols were approved by our institution's plan for research. Also, this research contains neither human nor animal studies.

Additional information
Correspondence and requests for materials should be addressed to A.A.A.E.-L. or B.A.-E.-A.