Received: 14 June 2023 | Revised: 27 September 2023 | Accepted: 6 October 2023

CAAI Transactions on Intelligence Technology

DOI: 10.1049/cit2.12292

ORIGINAL RESEARCH

# A novel medical image data protection scheme for smart healthcare system

Mujeeb Ur Rehman[1] | Arslan Shafique[2] | Muhammad Shahbaz Khan[3] | Maha Driss[4] | Wadii Boulila[4] | Yazeed Yasin Ghadi[5] | Suresh Babu Changalasetty[6] | Majed Alhaisoni[7] | Jawad Ahmad[3]

[1]School of Computer Science and Informatics, Cyber Technology Institute, De Montfort University, Leicester, UK

[2]Department of Biomedical Engineering, University of Glasgow, Glasgow, UK

[3]School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh, UK

[4]Robotics and Internet-of-Things Laboratory, Prince Sultan University, Riyadh, Saudi Arabia

[5]Department of Computer Science, Al Ain University, Al Ain, United Arab Emirates

[6]Department of Computer Engineering, College of Computer Science King Khalid University, Abha, Saudi Arabia

[7]Computer Sciences Department, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

**Correspondence**

Jawad Ahmad.
Email: J.Ahmad@napier.ac.uk

**Funding information**

King Khalid University, Grant/Award Number: RGP.2/379/44

## Abstract

The Internet of Multimedia Things (IoMT) refers to a network of interconnected multimedia devices that communicate with each other over the Internet. Recently, smart healthcare has emerged as a significant application of the IoMT, particularly in the context of knowledge-based learning systems. Smart healthcare systems leverage knowledge-based learning to become more context-aware, adaptable, and auditable while maintaining the ability to learn from historical data. In smart healthcare systems, devices capture images, such as X-rays, Magnetic Resonance Imaging. The security and integrity of these images are crucial for the databases used in knowledge-based learning systems to foster structured decision-making and enhance the learning abilities of AI. Moreover, in knowledge-driven systems, the storage and transmission of HD medical images exert a burden on the limited bandwidth of the communication channel, leading to data transmission delays. To address the security and latency concerns, this paper presents a lightweight medical image encryption scheme utilising bit-plane decomposition and chaos theory. The results of the experiment yield entropy, energy, and correlation values of 7.999, 0.0156, and 0.0001, respectively. This validates the effectiveness of the encryption system proposed in this paper, which offers high-quality encryption, a large key space, key sensitivity, and resistance to statistical attacks.

KEYWORDS

data analysis, medical image processing, security

## 1 | INTRODUCTION

The Internet of Multimedia Things (IoMT) is an extension of the Internet of Things that specifically involves interconnection, communication, and data transfer among different multimedia devices over the Internet. The IoMT is broad and can be applied to many different areas, one of which is smart healthcare. In smart healthcare, knowledge-based learning can play a significant role in enhancing the capabilities of the system. In this context, the medical imaging devices, particularly act as essential components of the smart healthcare system. In smart healthcare systems, IoMT, capture images, such as X-rays, MRIs (Magnetic Resonance Imaging), or CT scans (Computed Tomography Scans), and transmit them over the Internet to a specific destination (hospital or doctor's office). The transmission of this sensitive medical imaging data over insecure Internet channel poses significant risks as attackers can potentially manipulate or steal this information [1, 2], thereby jeopardising patient safety. Securing medical imaging data is crucial, particularly given the sensitive information inside these digital images [3]. Although the transmission of digital data via email is generally considered safe, it may not provide sufficient data privacy; hence, an image encryption method is needed to be used to secure sensitive data developed to ensure secure transmission of MRI images. To secure this information, the use of image encryption is a preferred technique that protects patients' data privacy [4].

In addition to security concerns, the transmission of high-quality medical imaging may exert a burden on the limited bandwidth of the Internet channels. Hence, there is an indispensable need for encryption schemes that not only ensure the security of transmitted medical data but are also lightweight, energy-efficient, and computationally efficient [5]. These attributes are crucial for facilitating seamless transmission over wireless channels with minimal delay, complexity, and resource consumption. Traditionally, digital photos are encrypted using the conventional and established encryption techniques, that is, RSA, data encryption standard, blowfish, and advanced encryption standard, etc [6–9]. Normally, the encryption schemes that employ multiple encryption rounds don't deem fit in real-time encryption scenarios because they consume a lot of time to encrypt images, despite their ability to provide a sufficient level of security. Conventional encryption schemes are primarily suitable for encrypting bits and textual data. Hence, this paper proposes an encryption scheme for medical images (ESMI) that utilise bit-plane extraction and chaos theory. The technique presented in this paper is tailored to reduce the correlation between pixels in medical images. Several X-ray, CT, and MRI images are selected and encrypted using the proposed work.

### 1.1 | Overview of the proposed encryption technique

In the proposed encryption technique, eight-bit medical images of size $M$(Rows) × $N$ are chosen for encryption. Initially, to decompose the input image into its sub-band frequencies, the DWT (Discrete Wavelet Transform) is employed. This helps in expediting the encryption procedure and minimise the duration required for it. Once the frequency sub-bands have been broken down, only the sub-band with low frequency is then encrypted because it contains most of the information. Moreover, the low-frequency sub-bands are further broken down into eight-bit planes. This results in low encryption time and ensures effective protection. According to Tang et al. [10], bit plane encryption is more secure than pixel encryption.

The rows and columns of pixel values of the first four bit-planes (Most significant bit-planes) are scrambled. Two random sequences are generated using a chaotic Henson map for scrambling image pixel values. By directly permuting or scrambling image pixels, the histogram of the scrambled image is never altered. A key benefit of scrambling the pixel values at the bit level is that the histogram of the scrambled image also gets scrambled along.

After the bit-plane scrambling, the diffusion phase begins, which consists of two fundamental operations: (a) substitution boxes and (b) exclusive OR operation (XOR). The pixel values have been substituted with the values of the substitution boxes by following the process explained in [11]. For the XOR, a random two-dimensional image of size $M \times N$ is generated by selecting the appropriate initial condition of the chaotic map.

As this paper focuses on the encryption of multiple images, three different medical images are chosen simultaneously: a CT scan, an MRI scan, and an X-ray for encryption. After encrypting the images they are merged together to create the final encrypted image. A generalised framework of the scheme proposed in this paper is depicted in Figure 1.

## 2 | RELATED WORK

Medical images have a strong correlation between neighbour pixels, but the present encryption algorithms may not provide adequate levels of security to effectively encrypt the images. [12, 13]. This is why researchers tend to come up with highly reliable image encryption algorithms. In recent years, numerous encryption approaches, including transformation encryption, optical encryption, chaos, and bit-plane extraction-based encryption, have been proposed to secure medical images from several cyberattacks such as malware, man-in-the-middle, and brute force attacks [14, 15]. Among such encryption techniques, chaos and bit-plane extraction-based encryption systems have captured the interest of researchers.

Chaotic cryptosystems have been developed due to their enamouring features such as unpredictability, sensitivity to secret keys, ergodicity, and the ability to produce pseudo-random sequences [16, 17]. The development of a chaos-based encryption technique is uncomplicated, but it offers a high level of security.

To secure medical images, a two-phase image encryption algorithm is presented in [18]. It consists of two major phases; (a) key generation based on chaos and (b) diffusion using DNA encoding. Before applying diffusion and confusion processes using chaos, the hashing function is deployed on the plaintext medical images. Next, the confusion phase involves the utilisation of the zigzag chaotic map and the Bernoulli shift map. After the confusion process, diffusion processes are incorporated using the XOR, which is applied to the plaintext medical image and a mask image generated using the chaotic map. All such operations are applied sequentially. Therefore, the time required to execute these operations is around 4.56 s which is quite high in real-time scenarios.

A two-stage encryption algorithm has been proposed in [14]. The authors named it as ‘double phase image encryption

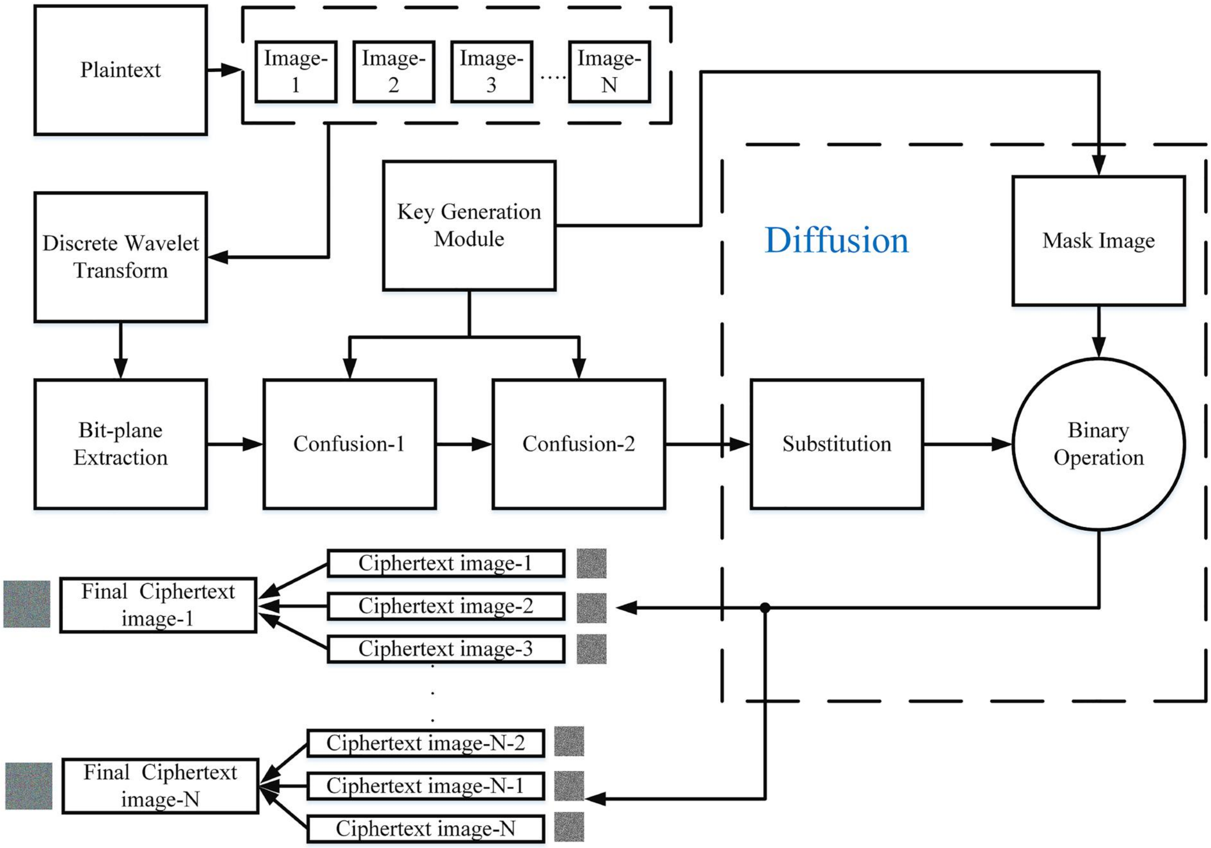


**FIGURE 1** Overview of the proposed framework.

(DPIE)'. In the first stage, the plaintext image is substituted with the values generated using DNA coding. In addition, once the original image has been substituted with the encrypted version, it is split into various distinct blocks. Then, a random sequence was generated using a chaotic logistic map. The sequence is carefully generated by selecting suitable initial conditions and control parameters. To further enhance the security of medical images, the initial conditions used in the chaotic map are encrypted using RSA to provide an additional layer on the secret keys. During the second stage, confusion is created between the pixels of the first stage images. This manipulated image is given the name pre-ciphered image. Lastly, to create diffusion, an XOR is applied. Based on the evaluation, the performance of DPIE is suitable for securing medical images. The only vulnerability that exists in DPIE is the computational complexity. In [19], it is claimed that any plaintext image of size 256 × 256 takes around 20 s to substitute all the image pixels. As the substitution process is included in DPIE in which all the image pixels are altered, also other operations such as confusion diffusion and XOR are performed, and the total encryption duration for a 256 × 256 image may exceed 20 s, making it unsuitable for real-time applications.

Moreover, a DNA encryption scheme has been presented in [20]. In this scheme, the plaintext image has been utilised to calculate a 256-bit hash value. The new initial conditions and control parameters are determined by this hash. These initial conditions and control parameters are kept as secret keys. Therefore, for every different plaintext image, the secret keys are different, which enhances image security. Once the values of secret keys are calculated, a random sequence is determined by implementing the chaotic map. This random sequence helps in permuting the pixels of the plaintext image. After pixel permutation, DNA-based permutation of rows and columns is performed, which helps to produce randomness. Lastly, a final encrypted image is generated by using the XOR operation.

Ibrahim et al. introduced a medical image encryption method in [21] that utilises a substitution box (S-box) and chaotic behaviour. Instead of utilising multiple S-boxes, the authors proposed the adoption of a single S-box. Anees et al. [22] discussed how to mitigate the risks associated with employing a single S-box. Using only one S-box is not enough to effectively replace a pixel in an image and ensure that the substituted image maintains the information. Therefore, the authors proposed that more s-boxes should be utilised. According to the experimental findings, the encryption method based on multiple S-boxes performs better than the method that uses a single S-box. However, it does not offer sufficient protection to digital images to withstand statistical attacks. In addition, a cryptographic solution is presented in [11], in the presented technique the substituted image is generated using multiple substitution boxes and is broken down into blocks of size 8 × 8. They actually extended the idea of multiple s-boxes that was presented in [22], The statistical results exhibit that the upgraded version of the encryption scheme proposed in [22] provides better security performance and can resist statistical attacks.

In [23], Guesmi et al. extend the idea proposed in [21] and used DNA and hash algorithm SHA-2 in their proposed ESMI. The authors employ a hybrid chaotic map as the only distinctive element in their encryption approach. The rationale for using a multi-dimensional chaotic map instead of a single dimension chaotic map is to improve the encryption scheme as a whole in security perspective. The method of using DNA and SHA-2 is the same as adopted in [21]. However, the hyperchaotic map provides better security than the encryption algorithm proposed in [21]. Although the ESMI offers better security, it is unsuitable for real-time encryption scenarios. From previous literature, it is clear that multi-dimensional chaotic map takes more computational time than a single dimension chaotic map. Therefore, The ESMI is not better as compared to the scheme presented in [21] in terms of computational complexity.

In most of the existing schemes, a significant problem of computational complexity must be overcome to use the encryption algorithms in real-time applications. Moreover, the substitution box-based encrypting scheme has vulnerabilities of not properly concealing image pixels and high computational complexity. Therefore, chaotic maps, multiple S-boxes, and bit-plane extraction techniques are used to overcome such issues. To achieve the desired purpose, the following contributions have been made in this paper.

- In this encryption technique, the bit-planes of the medical images are extracted and only the most significant ones, which contain the majority of the original image's information, are encrypted. This approach reduces the amount of processing time needed for encryption.
- Permutation is performed on the bit-plane, which alters its histogram and distinguishes it from the original image. It has been proven previously that simply permuting the image pixels would result in a permuted image that would have an identical histogram as that of the original image. This paper disproves that claim.
- For enhanced security, a multi-dimensional chaotic map has been employed to induce both confusion and diffusion.
- Extensive experimentation has also been performed to validate the effectiveness of the proposed technique by calculating several key evaluation parameters, that is, energy, contrast, correlation, entropy, etc.
- A brute-force-attack has also been employed to show that it is difficult for the attacker to find out all the possible combinations of the secrete to decrypt the original information. Moreover, the noise and the cropping attack have also been performed to prove that the encryption technique is resistant to noise and cropping attacks.

The subsequent parts of this paper are organised as follows: Section 3 provides the necessary preliminaries and prerequisites for the proposed encryption scheme. Section 4 describes the proposed encryption scheme in detail. In Section 5, we present the results and experimental findings. Finally, Section 6 concludes the paper by summarising the proposed work and offering some suggestions for future research.

## 3 | PRELIMINARIES

To ensure adequate security and reduce the computational time required for encryption, the proposed work incorporates the following cryptographic components.

- Chaotic maps
- Transformation using discrete wavelets (The DWT method)
- Bit-plane extraction

### 3.1 | Chaotic maps utilised in this research

The suggested approach employs two distinct chaotic maps, that is, a single-dimension Logistic chaotic map, and a two-dimension Henon map. [24, 25]. The mathematical expressions for both the chaotic maps are given in Equations (1) and (2) respectively.

$$\left(\mathbf{T}_{N+1},\mathbf{Q}_{N+1}\right) = \left\{\begin{matrix} 1 - \Gamma \times \left(\mathbf{T}_N^2\right) + \mathbf{Q}_N \\ \Xi \times \mathbf{T}_N^2 \end{matrix}\right\} \tag{1}$$

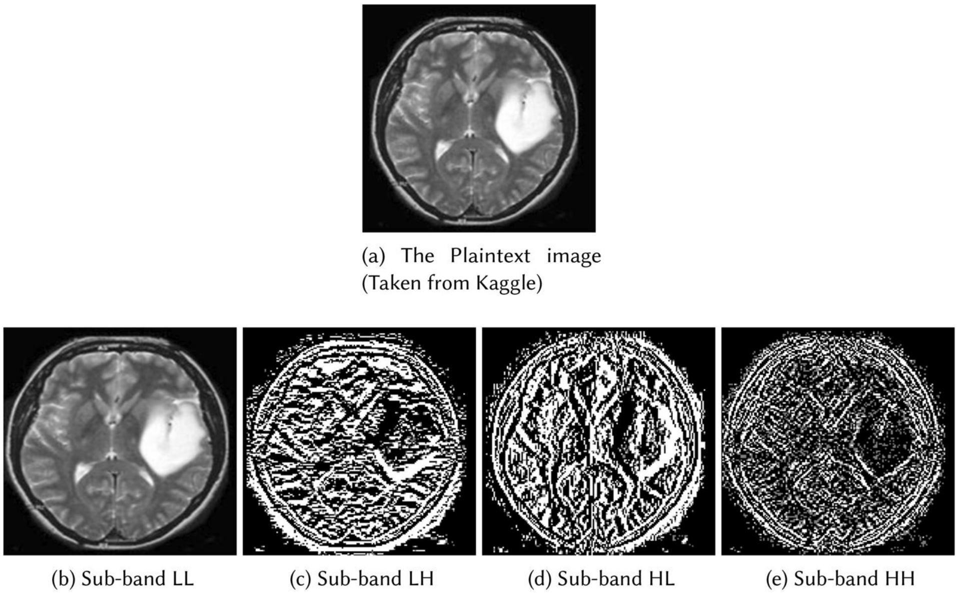
$$\Psi_{N+1} = \Upsilon_N \Omega (1 - \Omega_N) \tag{2}$$

where $\mathbf{T_0}$ and $\mathbf{Q_0}$ tend to be the state variables and $\Gamma$ and $\Xi$ are the system parameters of Henon map. The Henon map can generate two different chaotic sequences simultaneously such as $\mathbf{T} = \mathbf{T}_1, \mathbf{T}_2, \mathbf{T}_3, \ldots, \mathbf{T}_N$ and $\mathbf{Q}_n = \mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3, \ldots, \mathbf{Q}_N$.

$\Gamma$ and $\Xi$ are the initial condition and control parameter respectively. The chaotic logistic map can generate only a single random sequence at a time such as $\Gamma = \Gamma_1, \Gamma_2, \Gamma_3 \cdots, \Gamma_N$. These sequences are used to permute the rows and columns of the original medical image to break the correlation between the image pixels.

### 3.2 | Discrete wavelet transform—DWT

A signal can be transformed into its wavelet components using a wavelet transform [26]. Large and tiny wavelets may distinguish between a signal's fine and coarse features. In order to isolate and capture fine details at a small scale, it is necessary to use small wavelets. On the other hand, large wavelets are used to separate the most important features. [27]. In this paper, the plaintext image is broken down into four frequency sub-bands (HH sub-band, HL sub-band, LH sub-band, and LL sub-band) by using the Haar wavelet transform. In wavelet


(a) The Plaintext image (Taken from Kaggle)

(b) Sub-band LL (c) Sub-band LH (d) Sub-band HL (e) Sub-band HH

**FIGURE 2** Frequency sub-bands of plaintext image.

decomposition, the LL sub-band typically carries most of the original image's information, while the other sub-bands are responsible for capturing finer details such as edges as shown in Figure 2.

The expression $P' = HOH^{y}$ is used to express the Haar wavelets. Here, $O$ is the plaintext image, $H$ is the Haar matrix and $P$ represents the Haar basis functions $(h_{\alpha}(\omega))$. Where $\omega \in [01]$ and $\alpha$ is defined as $\alpha | \alpha \in N \wedge 0 \leq \alpha \leq M - 1$. Uniquely, it may be broken as follows:

$$\alpha = 2^{\beta} + q \tag{3}$$

where $\beta$ is the maximum power of 2 and $q$ is the remainder which is $q = 2^{\beta} - \alpha$ respectively. The Haar basis function can be defined using Equation (4).

$$h_{\alpha}(\omega) = \frac{1}{\sqrt{M}} \begin{cases} 1 & if \alpha = 0 \quad \& \quad 0 \leq \omega < 1 \\ 2^{\beta/2} & if \alpha > 0 \quad \& \quad t/2^{\beta} \leq \omega < \dfrac{q+0.5}{2^{\beta}} \\ -2^{\beta/2} & if \alpha > 0 \quad \& \quad (q+0.5)/2^{\beta} \\ & \quad \leq w < \dfrac{q+1}{2^{\beta}} \\ 0 & \text{Elsewhere} \end{cases} \tag{4}$$

Equation (5) shows that the 2-dimensional Haar wavelet transform (2HWT) can be derived using the inverse of the transformation kernel.

$$h'(\omega,\alpha) = \frac{1}{\sqrt{M}} h_{\alpha}(\omega/M) \qquad \omega = 0,1,2,\ldots,M-1 \tag{5}$$

where, $h_{\alpha}(\omega)$ is defined as:

$$h_{\alpha}(\omega) = H' \\ = \begin{cases} h_0\left(\dfrac{0}{M}\right) & h_0\left(\dfrac{1}{M}\right) & \ldots h_0\left(\dfrac{M-1}{M}\right) \\ h_1\left(\dfrac{0}{M}\right) & h_1\left(\dfrac{1}{M}\right) & \ldots h_1\left(\dfrac{M-1}{M}\right) \\ h_2\left(\dfrac{0}{M}\right) & h_2\left(\dfrac{1}{M}\right) & \ldots h_2\left(\dfrac{R-1}{M}\right) \\ . & . & . \\ . & . & . \\ . & . & . \\ h_{M-1}\left(\dfrac{0}{M}\right) & h_{M-1}\left(\dfrac{1}{M}\right) & \ldots h_{M-1}\left(\dfrac{R-1}{M}\right) \end{cases} \tag{6}$$

The resultant transformation matrix for $\alpha = 0, 1, 2, \ldots, M - 1$ is given in Equation ??

$$H = \frac{1}{\sqrt{M}} H' \tag{7}$$

In the case of digital images I(A, B), which are two-dimensional, both low and high pass filters are used to analyse the pixel rows in the horizontal direction and calculate the output in the two-dimensional image ($L_f$ and $H_f$) having a size of $\frac{A}{2} \times \frac{B}{2}$. After that, both filters will be used to analyse the pixel columns in the vertical direction and produce an output in the images ($L_f$ and $H_f$).

## 3.3 | Bit-plane extraction

Bit plane extraction refers to the process of breaking down a plaintext image into a specific number of bit-planes [28]. A certain number of bit planes means how many bits are present in an image. For instance, the 8-bit image will have eight-bit planes. Similarly, a binary image will have two binary bit planes. In the proposed work, grayscale medical images are used, which are of eight bits. Therefore, after the extraction of bit planes from the medical image, as shown in Figure 3, there will be eight different bitplanes. The extracted eight bitplanes corresponding to the image displayed in Figure 3a are shown in Figure 3b–i, in which it can be seen that the first four bit planes, which are the least significant bits (Figure 3e–h) contain little information of the plaintext medical image. Whereas the most significant bitplanes contain most of the plaintext image information.

Different amounts of information present in an image can be calculated using Equation (8) [29].

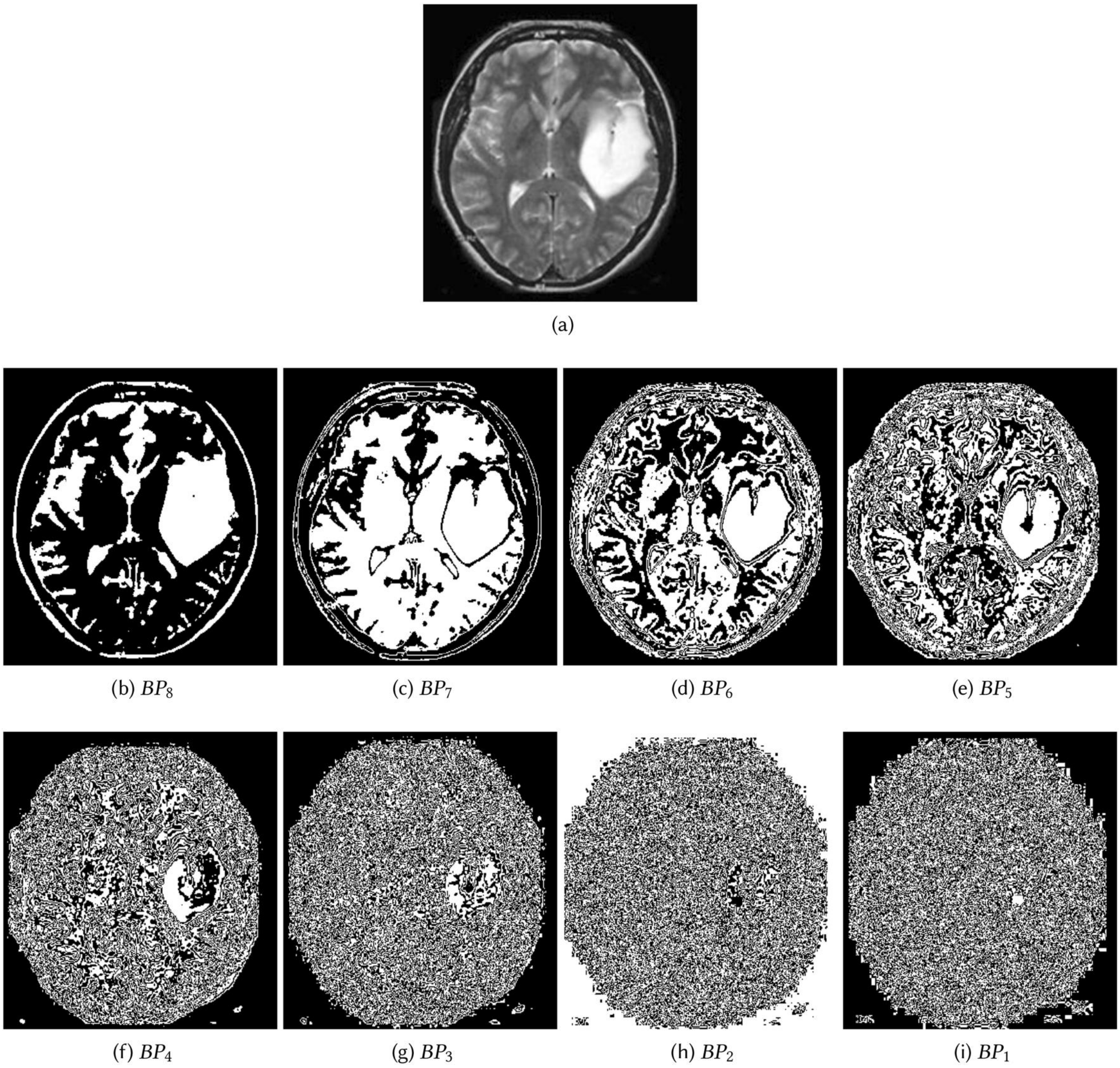
$$B_i = \frac{2^{i-1}}{\sum_{i=0}^{7} 2^{i-1}} \qquad i = 0,1,\ldots,7 \tag{8}$$

where $B_i$ represents the level of bit-plane. The percentage amount of information of the original medical image is displayed in Table 1.

Table 1 demonstrates that the most significant bit-planes contain more than 90% of the original information. Therefore, in order to speed up the encryption process, the majority

**TABLE 1** Amount of information in bit planes.

| *i* | Bit-plane position (Bi) | Information percentage present in an individual BPs |
|---|---|---|
| 0 | **BP$_1$** | 0.30 |
| 1 | **BP$_2$** | 0.79 |
| 2 | **BP$_3$** | 1.42 |
| 3 | **BP$_4$** | 3.12 |
| 4 | **BP$_5$** | 6.25 |
| 5 | **BP$_6$** | 12.23 |
| 6 | **BP$_7$** | 25.7 |
| 7 | **BP$_8$** | 50.20 |



(a)

(b) $BP_8$ (c) $BP_7$ (d) $BP_6$ (e) $BP_5$

(f) $BP_4$ (g) $BP_3$ (h) $BP_2$ (i) $BP_1$

**FIGURE 3** Bi-planes of the medical image: (a) Original (Plaintext) image, (b–e) Most significant bit-planes, (f–i) least significant bit-planes.

of encryption steps concentrate on these bit-planes. On the other hand, the permutation operation is exclusively used to break the correlation between pixel values in the least significant bit-planes.

## 4 | PROPOSED ENCRYPTION SCHEME

The proposed encryption has four main ingredients: (a) DWT, (b) the Bit plane extraction, (c) Bit-level Permutation, (d) Diffusion using XOR and substitution. The overview of the scheme adopted in this paper is given in Figure 4.

Before, encrypting the medical images, several keys are generated using the key generation module.

### 4.1 | Key generation module

The steps to generate secret keys are given in Algorithm 1.

**Algorithm 1 Algorithm for secrete key generation**

```
Input Seed values: $x_0$, $y_0$, $\mu$ and $Z_0$
    for $N = 1{:}1000$;
Initialise Henon map
        $(\mathbf{T}_{N+1}, \mathbf{Q}_{N+1}) = \begin{Bmatrix} 1 - \mathbf{\Gamma} \times (\mathbf{T}_N^2) + \mathbf{Q}_N \\ \mathbf{\Xi} \times \mathbf{T}_N^2 \end{Bmatrix}$
Initialise logistic map
        $\mathbf{\Psi}_{N+1} = \mathbf{Y}_N \mathbf{\Omega}(1 - \mathbf{\Omega}_N)$
Multiple each value stored in $\mathbf{T_N}$ and $\mathbf{Q_N}$ with a large integer number to amplify them as follows:
        $\begin{Bmatrix} \mathbf{T}_u(N) = (\mathbf{T}_{N+1}) \times 999; \\ \mathbf{Q}_u(N) = (\mathbf{Q}_{N+1}) \times 999; \end{Bmatrix}$
        $\boldsymbol{\Psi} = \boldsymbol{\Psi}_{N+1} \times 999;$
Discard the digits at right of the decimal point as follows:
        $\begin{Bmatrix} \mathbb{Z}\{\mathbf{T}_{int}(N)\} = \mathrm{floor}(\mathbf{T}_u(N)) \\ \mathbb{Z}\{\mathbf{Q}_{int}(N)\} = \mathrm{floor}(\mathbf{Q}_u(N)) \end{Bmatrix}$
        $\mathbb{Z}\{\mathbf{\Psi}_{int}(N)\} = \mathrm{floor}(\mathbf{\Psi}(N)$
Take modulo to restrict the values of $\mathbb{Z}\{\mathbf{T}_{int}(N)\}$ and $\mathbb{Z}\{\mathbf{Q}_{int}(N)\}$ in the range $[0\ 255]$
        $\begin{Bmatrix} \mathbf{MT}(N) = \mathrm{mod}(\mathbb{Z}\{\mathbf{T}_{int}(N)\}, 256) \\ \mathbf{MQ}(N) = \mathrm{mod}(\mathbb{Z}\{\mathbf{Q}_{int}(N)\}, 256) \end{Bmatrix}$
        $\mathbf{M\Psi}(N) = \mathrm{mod}(\mathbb{Z}\{\mathbf{M\Psi}_{int}(N)\}, 256)$
    end
Choose first 256 unique values from the values stored in $\mathbf{MT}(N)$ and $\mathbf{MQ}(N)$ as follows:
        $\begin{Bmatrix} Key_{\mathbf{T}} = \mathrm{unique}(\mathbf{MT}, '\mathrm{stable}') \\ Key_{\mathbf{Q}} = \mathrm{unique}(\mathbf{MQ}, '\mathrm{stable}') \end{Bmatrix}$
        $Key_{\boldsymbol{\Psi}} = \mathrm{unique}(\boldsymbol{M\Psi}, '\mathrm{stable}')$
Output random sequences ($Key_{\mathbf{T}}$, $Key_{\mathbf{Q}}$ and $Key_{\mathbf{\Psi}}$) for permutation purposes.
```

A stepwise explanation of the proposed encrypting process is given below:

- Multiple two-dimensional plaintext images $P_1(i, j)$, $P_2(i, j)$, $P_3(i, j)$, $\cdots P_N(i, j)$ are given as input to the proposed encryption algorithm. Where $i$ and $j$ correspond to the row and column numbers of the plaintext image respectively.
- Decompose the plaintext images into its four frequency sub-bands $[(\mathbf{LL}_{im_1}, \mathbf{LH}_{im_1}, \mathbf{HL}_{im_1} \mathbf{HH}_{im_1})$, $(\mathbf{LL}_{im_2}, \mathbf{LH}_{im_2}, \mathbf{HL}_{im_2}, \mathbf{HH}_{im_N}) \cdots (\mathbf{LL}_{im_N}, \mathbf{LH}_{im_N}, \mathbf{HL}_{im_N}, \mathbf{HH}_{im1})]$. Where, $\mathbf{LL}_{im_1}$,$\mathbf{LL}_{im_2}$ and $\mathbf{LL}_{im_N}$ represents the Low frequency sub-bands extracted from the $image_1(im_1)$, $image_1(im_2)$ and $image_1(im_N)$ respectively. Among such frequency sub-bands, only low frequency bands $\mathbf{LL}_{im_1}$, $\mathbf{LL}_{im_2}, \cdots \mathbf{LL}_{im_N}$ and considered for encryption. Figure 2b shows that the low-frequency subbands contain maximum information. Therefore, encrypting low-frequency bands results in expediting the encryption process.
- Take DWT of $\mathbf{LL}_{im_i}$ for three times. Every four sub-bands corresponding to each $\mathbf{LL}_{im_i}$ will be:

$$\text{Sub-bands of } \mathbf{LL}_{im_1} = \begin{cases} DWT(\mathbf{LL}_{im_1}) \rightarrow [\mathbf{LL}_{1im_1}, \mathbf{LH}_{1im_1}, \mathbf{HL}_{1im_1}, \mathbf{HH}_{1im_1}], \\ DWT(\mathbf{LL}_{1im_1}) \rightarrow [\mathbf{LL}_{2im_1}, \mathbf{LH}_{2im_1}, \mathbf{HL}_{2im_1}, \mathbf{HH}_{2im_1}], \\ DWT(\mathbf{LL}_{2im_1}) \rightarrow [\mathbf{LL}_{3im_1}, \mathbf{LH}_{3im_1}, \mathbf{HL}_{3im_1}, \mathbf{HH}_{3im_1}], \\ DWT(\mathbf{LL}_{3im_1}) \rightarrow [\mathbf{LL}_{4im_1}, \mathbf{LH}_{4im_1}, \mathbf{HL}_{4im_1}, \mathbf{HH}_{4im_1}], \end{cases} \tag{9}$$

$$\text{Sub-bands of } \mathbf{LL}_{im_2} = \begin{cases} DWT(\mathbf{LL}_{im_2}) \rightarrow [\mathbf{LL}_{1im_2}, \mathbf{LH}_{1im_2}, \mathbf{HL}_{1im_2}, \mathbf{HH}_{1im_2}], \\ DWT(\mathbf{LL}_{1im_2}) \rightarrow [\mathbf{LL}_{2im_2}, \mathbf{LH}_{2im_2}, \mathbf{HL}_{2im_2}, \mathbf{HH}_{2im_2}], \\ DWT(\mathbf{LL}_{2im_2}) \rightarrow [\mathbf{LL}_{3im_2}, \mathbf{LH}_{3im_2}, \mathbf{HL}_{3im_2}, \mathbf{HH}_{3im_2}], \\ DWT(\mathbf{LL}_{3im_2}) \rightarrow [\mathbf{LL}_{4im_2}, \mathbf{LH}_{4im_2}, \mathbf{HL}_{4im_2}, \mathbf{HH}_{4im_2}], \end{cases} \tag{10}$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\text{Sub-bands of } \mathbf{LL}_{im_N} = \begin{cases} DWT\left(\mathbf{LL}_{im_N}\right) \rightarrow \left[\mathbf{LL}_{\mathbf{1}im_N}, \mathbf{LH}_{\mathbf{1}im_N}, \mathbf{HL}_{\mathbf{1}im_N}, \mathbf{HH}_{\mathbf{1}im_N}\right], \\ DWT\left(\mathbf{LL}_{\mathbf{1}im_N}\right) \rightarrow \left[\mathbf{LL}_{\mathbf{2}im_N}, \mathbf{LH}_{\mathbf{2}im_N}, \mathbf{HL}_{\mathbf{2}im_N}, \mathbf{HH}_{\mathbf{2}im_N}\right], \\ DWT\left(\mathbf{LL}_{\mathbf{2}im_N}\right) \rightarrow \left[\mathbf{LL}_{\mathbf{3}im_N}, \mathbf{LH}_{\mathbf{3}im_N}, \mathbf{HL}_{\mathbf{3}im_N}, \mathbf{HH}_{\mathbf{3}im_N}\right], \\ DWT\left(\mathbf{LL}_{\mathbf{3}im_N}\right) \rightarrow \left[\mathbf{LL}_{\mathbf{4}im_N}, \mathbf{LH}_{\mathbf{4}im_N}, \mathbf{HL}_{\mathbf{4}im_N}, \mathbf{HH}_{\mathbf{4}im_N}\right], \end{cases} \tag{11}$$

The size of each sub-band is reduced to one third. For instance, if the size of $\mathbf{LL}_{im_i}$ is 128 × 128, the dimensions of $\mathbf{LH}_{\mathbf{4}im_N}$ will be 16 × 16.

- Extract bit-planes from $\mathbf{LL}_{im_i}$. From each $\mathbf{LL}_{im_i}$, eight bit-panes are extracted. In the proposed work, three plaintext images are taken as inputs. Therefore, twenty four bit-planes $[\left(\mathbf{BP}_{\mathbf{1}im_1}, \mathbf{BP}_{\mathbf{2}im_1}, \ldots, \mathbf{BP}_{\mathbf{8}im_1}\right)$, $\left(\mathbf{BP}_{\mathbf{1}im_2}, \mathbf{BP}_{\mathbf{2}im_2}, \ldots, \mathbf{BP}_{\mathbf{8}im_2}\right)$, $\left(\mathbf{BP}_{\mathbf{1}im_3}, \mathbf{BP}_{\mathbf{2}im_3}, \ldots, \mathbf{BP}_{\mathbf{8}im_3}\right)]$ are extracted from three input plaintext images.
- Permute the row and columns of the Most significant bit-planes [($\mathbf{BP}_{\mathbf{8}im_1}$, $\mathbf{BP}_{\mathbf{7}im_1}$, $\mathbf{BP}_{\mathbf{6}im_1}$, $\mathbf{BP}_{\mathbf{5}im_1}$), ($\mathbf{BP}_{\mathbf{8}im_2}$, $\mathbf{BP}_{\mathbf{7}im_2}$, $\mathbf{BP}_{\mathbf{6}im_2}$, $\mathbf{BP}_{\mathbf{5}im_2}$), ($\mathbf{BP}_{\mathbf{8}im_3}$, $\mathbf{BP}_{\mathbf{7}im_3}$, $\mathbf{BP}_{\mathbf{6}im_3}$, $\mathbf{BP}_{\mathbf{5}im_3}$)]. For row and column permutation the secrete keys $\text{Key}_{\mathbf{T}}$ and $\text{Key}_{\mathbf{Q}}$ are used respectively. Using the permutation process, only the pixel's positions can be changed, but the pixels remain the same. Therefore, the Pixel permutation cannot resist statistical attacks such as entropy and histogram attacks. For example, Figure 5 shows the permuted bit planes having broken correlation between the image pixels, and hence, no information can be visualised.
- To further modify the pixel values, substitute them with the S-box proposed in [30].
- To generate the final encrypted images, the corresponding bit-planes ($P_i$) extracted from the noisy image ($\mathbf{B}_{N1}$, $\mathbf{B}_{N2}$, ⋯, $\mathbf{B}_{N8}$) are combined with the permuted bit-planes using an XOR. After the XOR operation, the pre-ciphered images ($\mathbf{E}'_1$, $\mathbf{E}'_2$, $\mathbf{E}'_3$, ⋯, $\mathbf{E}'_{24}$) are generated. The XOR operation is shown in Equations (12–14).
- Encrypted images are shown in Figure 6, which depicts that the proposed encryption scheme can encrypt the plaintext grayscale images simultaneously, but it generates a single encrypted image corresponding to three input images. The reason for using multiple input images is due to the capability of the proposed encryption algorithms to simultaneously encrypt three grayscale images or three colour images, treating each input as one colour component of a colour image. The proposed encryption scheme exhibits versatility in encrypting digital images of various formats,

$$\begin{gathered} \mathbf{E}'_1 = \sum_{a=1}^{R}\sum_{b=1}^{C} P_1(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N1}(i,j), \mathbf{E}'_2 = \sum_{a=1}^{R}\sum_{b=1}^{C} P_2(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N2}(i,j), \\ \cdots \mathbf{E}'_8 = \sum_{a=1}^{R}\sum_{b=1}^{C} P_8(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N8}(i,j) \end{gathered} \tag{12}$$

$$\begin{gathered} \mathbf{E}'_9 = \sum_{a=1}^{R}\sum_{b=1}^{C} P_1(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N1}(i,j), \mathbf{E}'_{10} = \sum_{a=1}^{R}\sum_{b=1}^{C} P_2(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N2}(i,j), \\ \cdots \mathbf{E}'_{16} = \sum_{a=1}^{R}\sum_{b=1}^{C} P_8(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N8}(i,j) \end{gathered} \tag{13}$$

$$\begin{gathered} \mathbf{E}'_{17} = \sum_{a=1}^{R}\sum_{b=1}^{C} P_1(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N1}(i,j), \mathbf{E}'_{18} = \sum_{a=1}^{R}\sum_{b=1}^{C} P_2(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N2}(i,j), \\ \cdots \mathbf{E}'_{24} = \sum_{a=1}^{R}\sum_{b=1}^{C} P_8(a,b) \oplus \sum_{a=1}^{R}\sum_{b=1}^{C} \mathbf{B}_{N8}(i,j) \end{gathered} \tag{14}$$

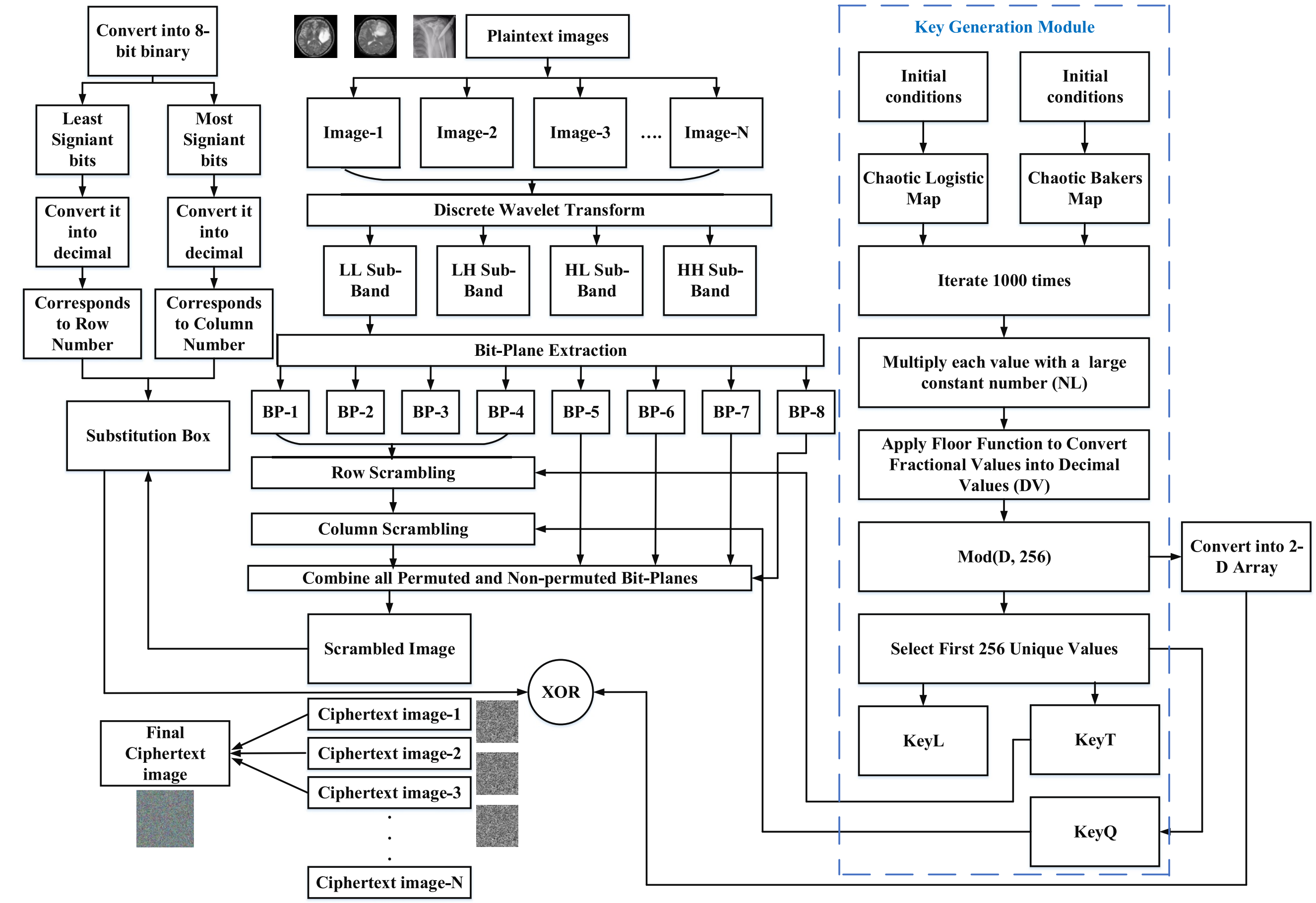
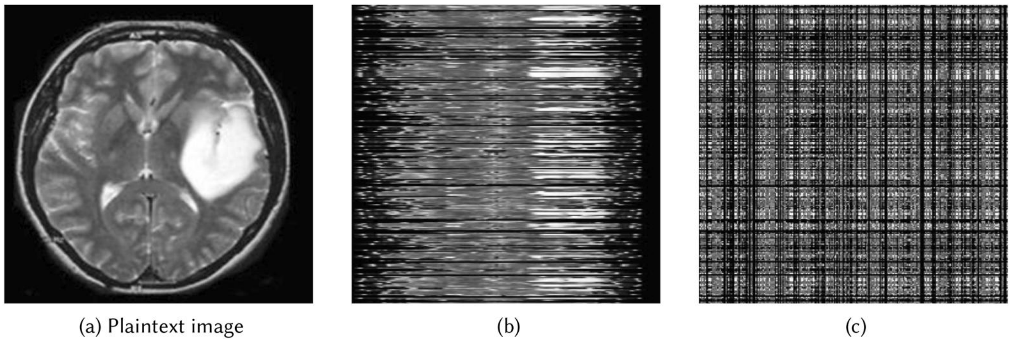


**FIGURE 4** Detailed block diagram of the proposed encryption scheme.


(a) Plaintext image

(b)

(c)

**FIGURE 5** Permuted images: (a) plaintext image, (b) Row scrambling, and (c) Column scrambling performed after row scrambling.

including jpg, png, etc. Additionally, beyond medical images, the proposed scheme can also encrypt images related to military, defence, and general categories, such as baboon, cameraman, lina, etc.

## 5 | RESULTS AND ANALYSIS

The proposed encryption method's effectiveness is evaluated through various security analyses, including correlation, energy, entropy, contrast, histogram, and homogeneity. These analyses are conducted on a system running Windows 11, equipped with an 8 GB RAM, 11th Gen Intel(R) Core(TM) i5-1135G7 processor, operating at 2.40 GHz.

### 5.1 | Entropy as a measure of randomness in images

Entropy can be referred to as a measure of the level of randomness present in the pixels of an image. A higher level of randomness between image pixels results in a correspondingly higher entropy value as shown in Equation (15).

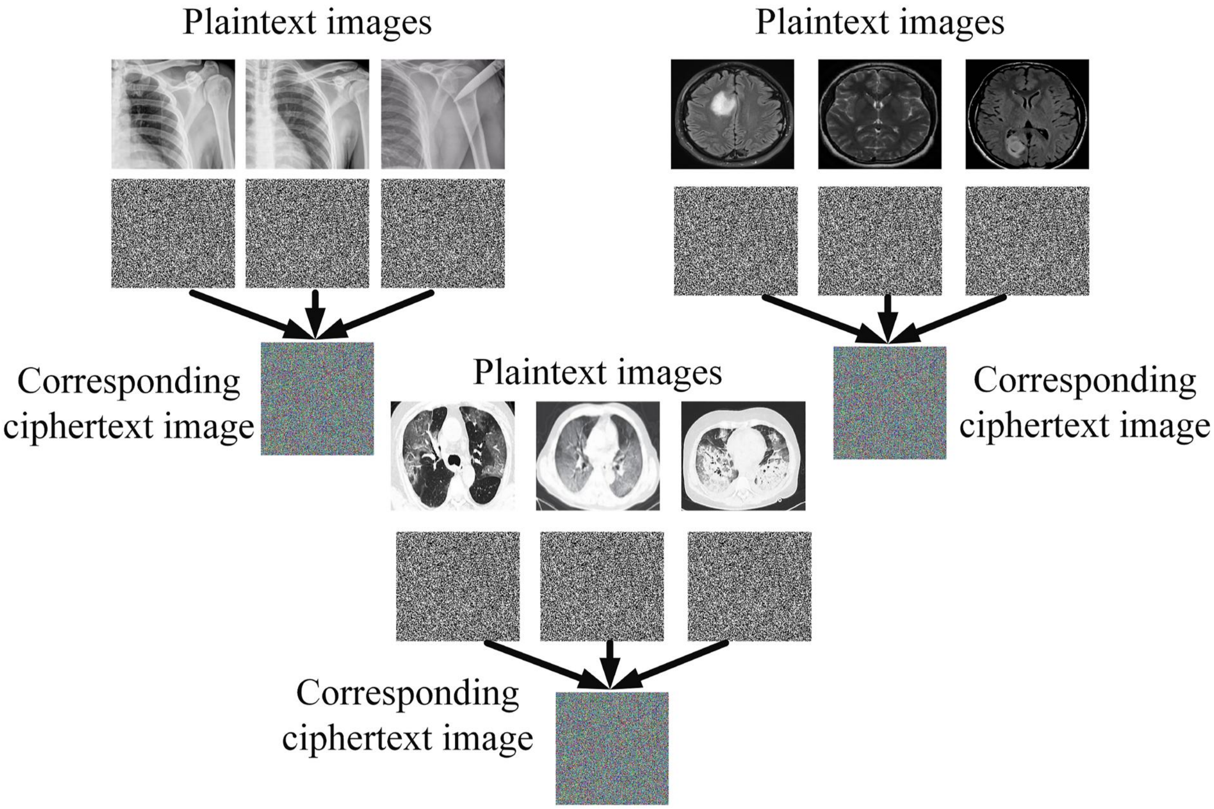

Plaintext images
Plaintext images
Corresponding ciphertext image
Plaintext images
Corresponding ciphertext image
Corresponding ciphertext image

**FIGURE 6** Plaintext images and their corresponding ciphertext images.

$$\text{Entropy} \propto Randomness \tag{15}$$

The optimal value for a given plaintext image may vary depending on how many bits an image contains, for example, an 8-bit image should have the optimal entropy value of 8. Similarly, the maximum entropy value of a binary image is 2. Entropy can be calculated by Equation (16)

$$\text{Entropy} = -\sum g(e_i)\log_2 g(e_i) \tag{16}$$

where: $g(e_i)$ denotes the probability of occurrence in the variable $e$.

The proposed work uses grayscale medical images of eight-bit to encrypt. Therefore, it is desired to obtain an entropy value close to 8. In addition, Table 2 displays a range of entropy values for different ciphertext images that were created using the proposed encryption method. This indicates that the proposed encryption system has the capability to generate entropy values that are close to eight.

## 5.2 | Energy as a metric of amount of information in images

The energy of an image refers to the level of information retained in an image. Higher levels of information present in images correspond to increased energy values, as shown in Equation (17).

**TABLE 2** Entropy analysis.

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| CT | 7.9887 | 7.9886 | 7.9886 | 7.9981 | 7.9994 |
| Tumour | 7.9788 | 7.9846 | 7.9788 | 7.9886 | 7.9989 |
| X-ray | 7.9986 | 7.9984 | 7.9887 | 7.9897 | 7.9997 |
| MRI | 7.9986 | 7.9976 | 7.9978 | 7.9964 | 7.9994 |
| CT scan | 7.9986 | 7.9946 | 7.9984 | 7.9967 | 7.9996 |

$$\text{Energy} \propto Information \tag{17}$$

The energy value of any image ranges from 0 to 1. A higher energy value corresponds to a large amount of information in an image. Therefore, it is always desired to obtain energy values close to zero in image encryption. The energy of any image can be calculated using Equation (18).

$$\text{Energy} = \sum I(r,c)^2 \tag{18}$$

where: $I(r, c)$ represents the pixel value placed at *rth* row and *cth* column.

Table 3 displays various energy values for different images. Table 3 depicts that the energy values of the encryption scheme proposed in this paper are much less than other encryption schemes in literature.

### 5.3 | Correlation analysis for similarity measurement of pixels

Correlation between image pixels shows the similarity between them. The higher similarity between the image pixels corresponds to the higher correlation value as shown in Equation (19).

$$\text{Correlation value} \propto \text{Similarity between image pixels} \qquad (19)$$

The value of image pixel correlation lies in the range [−1+1]. −1 shows the negative correlation between image pixels. A negative correlation means that if the value of the first pixel increases, the value of the neighbour pixel decreases. On the other hand, a positive correlation is opposite to the concept of a negative correlation. Correlation can be found using the following Equation (20)

$$CC = \frac{\mathrm{Cov}(r,c)}{\sigma_r \sigma_c} \qquad (20)$$

where,

$$\sigma_r = \sqrt{VARr}, \quad \sigma_c = \sqrt{VARc}$$

$$VAR(r) = \frac{1}{L}\sum\nolimits_{j=1}^{L}(r_i - E(r))^2,$$
$$\mathrm{Cov}(r,c) = \frac{1}{L}\sum\nolimits_{j=1}^{L}(r_i - E(r))\,(c_i - E(c))$$

$\sigma$ represents standard deviation, and $E$ is the expected value operator. Table 4 demonstrates that the proposed encryption system can break the correlation more effectively than the existing encryption schemes.

Furthermore, to figure out the correlation between the plaintext and ciphertext image pixels, several scattered plots are shown in Figure 7. The dots shown in Figure 7b–d are closer to each other exhibits high correlation between pixels in all directions such as horizontal, vertical and diagonal. However, Figure 7f–h shows the ciphertext image pixels correlation in horizontal, vertical and diagonal directions respectively. The dispersion of the dots indicates that the correlation between the ciphertext image pixels is much lower than that between the plaintext image pixels in all directions.

**TABLE 3** Energy analysis.

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| CT | 0.1632 | 0.0160 | 0.0160 | 0.0161 | 0.0157 |
| Tumour | 0.0160 | 0.0159 | 0.0159 | 0.0162 | 0.0156 |
| X-ray | 0.1613 | 0.0159 | 0.0160 | 0.061 | 0.0157 |
| MRI | 0.0160 | 0.0160 | 0.0159 | 0.0162 | 0.056 |
| CT scan | 0.0161 | 0.0159 | 0.0160 | 0.0162 | 0.0156 |

### 5.4 | Computational time analysis

In real-time applications, minimising time complexity is crucial, and it is important to keep the computational complexity of an encryption scheme as low as possible. To assess the time complexity of the proposed encryption algorithm, it was implemented using MATLAB 2014a, and the 'tic toc' command in MATLAB was utilised. The 'tic toc' command was used to encompass all mathematical and transformation operations in the proposed encryption method for time complexity calculations.

$$\text{tic} \rightarrow \text{Proposed encryption scheme} \rightarrow \text{toc}$$

Table 5 highlights the computational efficiency of the proposed work. As shown in Table 5, the time required to encrypt a 256 × 256 size plaintext image is lower for the proposed scheme compared to the existing scheme.

### 5.5 | Mean square error

Mean square error (MSE) is used to evaluate the difference between two images. Mathematically, MSE can be calculated using Equation (21).

$$\mathrm{MSE} = \frac{1}{RC}\sum_{i=1}^{R}\sum_{j=1}^{C}(P(i,j) - C(i,j))^2 \qquad (21)$$

The rows and columns of an image is represented by $R$ and $C$ respectively. Whereas, $P$(i,j) is the original image and $C(i,j)$ is an encrypted image.

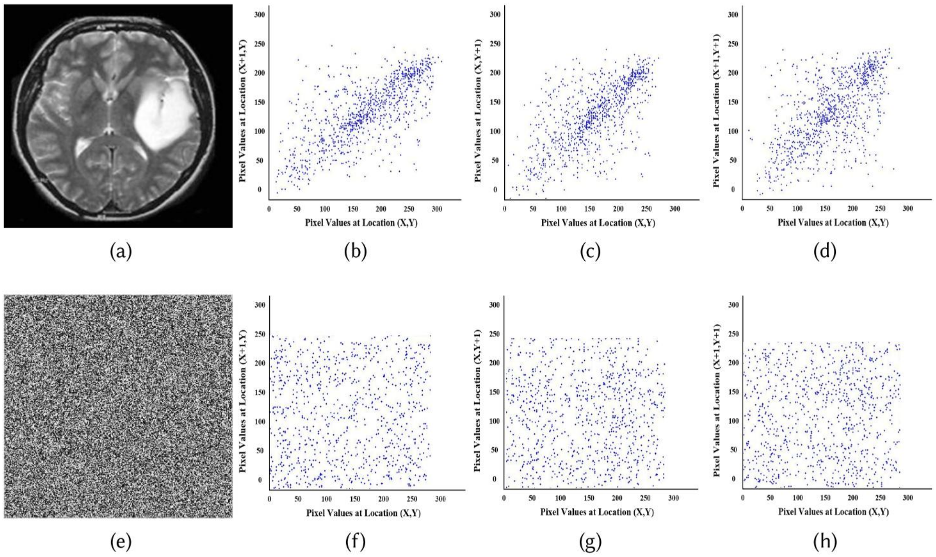
In an image encryption, MSE is frequently used to measure the difference between the pliantext and ciphertext images. More the difference between them, more stronger the encryption algorithm will be as given in Equation (22).

$$\mathrm{MSE} \propto \text{Security strength} \qquad (22)$$

In Table 6, the MSE values are given, which show that the error generated in the ciphertext image corresponds to the plaintext image is very high. In addition, the MSE values for the proposed work are more significant than the current ones, indicating that the proposed encryption algorithm performs better in MSE analysis than existing encryption schemes.

**TABLE 4** Correlation analysis.

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| CT | 0.0034 | 0.0035 | 0.0011 | −0.0013 | 0.0003 |
| Tumour | 0.0036 | 0.0037 | −0.0067 | −0.0077 | 0.0001 |
| X-ray | 0.0096 | 0.0065 | −0.0086 | 0.0011 | −0.0006 |
| MRI | 0.0060 | 0.0031 | 0.0010 | 0.0011 | −0.0001 |
| CT scan | 0.0013 | 0.0011 | 0.0010 | 0.0011 | 0.0004 |



(a) (b) (c) (d)

(e) (f) (g) (h)

**FIGURE 7** Correlation analysis of plaintext and encrypted images: (a) Plaintext image (b–d) Horizontal, vertical and diagonal correlation of plaintext image pixels, (e) Ciphertext image, (f–h) HOrizontal, vertical and diagonal correlation of corresponding ciphertext image pixels.

**TABLE 5** Computational time analysis (sec).

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| CT | 1.6454 | 1.3364 | 2.3365 | 1.1131 | 0.01358 |
| Tumour | 1.678 | 1.3365 | 1.6891 | 1.3365 | 0.03447 |
| X-ray | 1.6789 | 1.6654 | 1.3498 | 1.6431 | 0.0336 |
| MRI | 1.3664 | 1.6628 | 1.6798 | 1.6487 | 0.0919 |
| CT scan | 1.3678 | 1.6678 | 1.668 | 1.6789 | 0.06364 |

**TABLE 6** Mean square error analysis.

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| Images | 1265 | 1378 | 1336 | 1365 | 1467 |
| CT | 1247 | 1364 | 1302 | 331 | 1446 |
| Tumour | 1320 | 1310 | 1230 | 1223 | 1466 |
| X-ray | 1301 | 1229 | 1246 | 1304 | 1469 |
| MRI | 1203 | 1243 | 1276 | 1379 | 1490 |
| CT scan | 1276 | 1340 | 1394 | 1398 | 1469 |

## 5.6 | Quantification of PSNR

The Peak Signal-to-Noise Ratio (PSNR) is used to quantify the degradation between two pictures. PSNR is a commonly used metric in image encryption to measure the degree of similarity between the original and decrypted images. For the calculation of PSNR, it is mandatory to have the value of MSE for the desired images. The PSNR and MSE are inversely proportional to each other, as given in Equation (23).

$$\text{PSNR} = 20log_{10}\left(\frac{MAX_p}{\sqrt{MSE}}\right) \tag{23}$$

Here, the variable $MAX_p$ represents the maximum value that a plaintext image can possess.

Table 7 displays the PSNR values for both the proposed and existing encryption schemes. It is evident that the proposed scheme has the lowest PSNR value.

In addition to measuring the degradation between two images, PSNR can also be utilised to determine the amount of data loss during the recovery of the original image. Figure 8 shows the data loss analysis measured using PSNR. Figure 8c shows the decrypted image in which it can be seen that the decrypted and original images are identical, which means the value of PNSR will be infinity. This effect is shown in Figure 8d,e, in which a small portion of the plaintext and decrypted images are displayed, respectively. Both the portions of the images have no difference between the pixel values, demonstrating that the PSNR value will be infinity and there is no data loss after recovering the plaintext image.

## 5.7 | Analysing the key sensitivity

Key sensitivity refers to the minor change in the secret keys that leads to the major difference between the original and decrypted images. This paper utlizses four keys, that is, $x_0 = 0.130000000000000$, $y_0 = 0.350000000000000$, $\mu = 0.60000000000000$, $Z_0 = 0.320000000000000$. For the sensitivity analysis, each original key is added to a minor change ($\Delta = 10^{-15}$). The modified keys are $x_0' = x_0 + \Delta, y_0' = y_0 + \Delta$, $\mu' = \mu + \Delta, Z_0' = Z_0 + \Delta$. Such modified keys are then used to decrypt the plaintext image, as shown in Figure 9c, where the encrypted picture is distinguishable from the original plaintext image.

## 5.8 | Key space analysis

Keyspace analysis are frequently used to analysis the brute force attack and whether it can be affected by the encryption scheme or not. To launch the brute force attack, the eavesdropper tries all the possible combinations of the secret keys to find out the correct secret key in order to decrypt the original information. Therefore, the key space must be significant. The work that is being proposed makes use of four different keys, and the sensitivity of each key is $10^{-15}$, which indicates that each secret key has a key space of $10^{+15}$ 10 plus 15. Thus, the total key space for the secret keys utilised in the proposed work is $10^{+15*4}$, which is approximately equivalent to $2^{+213}$. According to Alvazair's claims, the key space needs to be about $2^{100}$. Also, the proposed method of encryption uses keys that are big enough to withstand a brute-force attack, and it meets the criteria for key-space set by Alvazair.

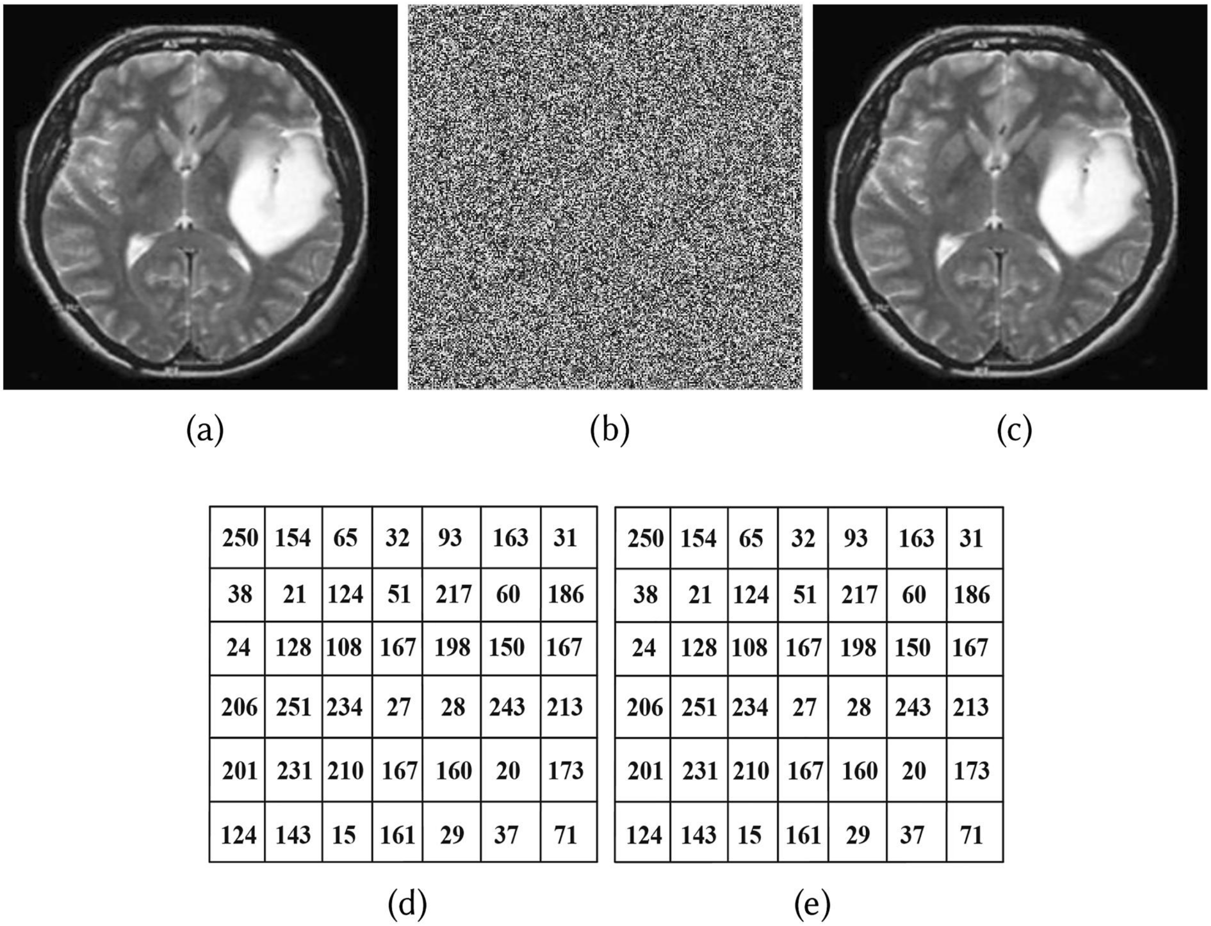
**TABLE 7** Peak signal to noise ratio analysis.

| Plaintext images | [31] | [32] | [33] | [34] | Proposed |
|---|---|---|---|---|---|
| CT | 23.6482 | 21.3279 | 23.1257 | 26.9987 | 13.4605 |
| Tumour | 26.3789 | 26.0148 | 23.6890 | 29.6781 | 10.3461 |
| X-ray | 29.6410 | 25.6784 | 28.6678 | 29.667 | 13.6655 |
| MRI | 28.6497 | 28.664 | 29.1056 | 28.678 | 12.3301 |
| CT scan | 23.6489 | 21.6491 | 23.0658 | 23.8970 | 11.0031 |

## 5.9 | Noise and cropping attack analysis

To make the decryption failure, the attackers often modify the encrypted images with some noise. An encryption scheme needs to have resistance against noise in order to withstand a noise attack. To analyse the noise attack, a random value $\delta$ is added as noise in each pixel value of the encrypted image as follows:

$$\begin{aligned} N_{im_1} &= C_1 + \delta \\ N_{im_2} &= C_2 + \delta \\ &\vdots \\ N_{im_N} &= C_N + \delta \end{aligned}$$



|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 250 | 154 | 65 | 32 | 93 | 163 | 31 |
| 38 | 21 | 124 | 51 | 217 | 60 | 186 |
| 24 | 128 | 108 | 167 | 198 | 150 | 167 |
| 206 | 251 | 234 | 27 | 28 | 243 | 213 |
| 201 | 231 | 210 | 167 | 160 | 20 | 173 |
| 124 | 143 | 15 | 161 | 29 | 37 | 71 |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 250 | 154 | 65 | 32 | 93 | 163 | 31 |
| 38 | 21 | 124 | 51 | 217 | 60 | 186 |
| 24 | 128 | 108 | 167 | 198 | 150 | 167 |
| 206 | 251 | 234 | 27 | 28 | 243 | 213 |
| 201 | 231 | 210 | 167 | 160 | 20 | 173 |
| 124 | 143 | 15 | 161 | 29 | 37 | 71 |

**FIGURE 8** Dataloss analysis of encrypted images: (a) plaintext image, (b) ciphertext image, (c) decrypted image, (d–e) Portion of plaintext and ciphertext images.

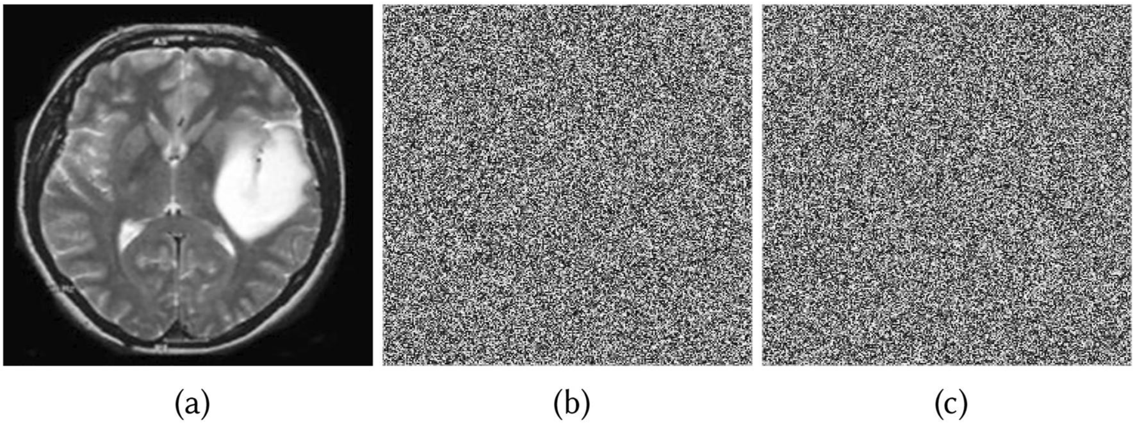


**FIGURE 9** Key sensitivity analysis of the proposed scheme: (a) plaintext image, (b) ciphertext image, (c) decrypted image with modified keys.

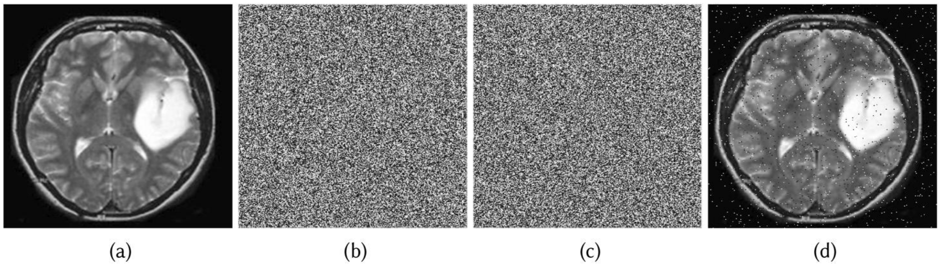


**FIGURE 10** Noise attack analysis of the proposed scheme: (a) Plaintext image (b) Encrypted image (c) Noisy version of the encrypted image (d) Decrypted of original image from noisy version of the encrypted image.

The plaintext, encrypted, and noisy image and its corresponding decrypted image are shown in Figure 10. From Figure 10d, it can be seen that the proposed encryption algorithm can recover the plaintext information with a bit of distortion, but the content of the original plaintext image can be visualised.

Apart from the noise attack, the eavesdropper crop a portion of the encrypted image to make the decryption failure. The encrypted and its corresponding cropped images are shown in Figure 11b,c respectively. The decrypted image can be visualised based on the information presented in Figure 11d. However, there is a little noise which can be negligible because the original information's content is clearly visible.

### 5.10 | Histogram analysis

A histogram of an image is a graphical representation of the distribution of pixel intensities in an image. It shows the frequency of occurrence of different intensity levels in the image. For example, an eight-bit image has 256 Gy levels. The frequency of grey levels can be represented by the peak mentioned in the histogram, as shown in Figure 12. In the case of enciphered images, a uniform and flat histogram is desirable, as it differs significantly from the histogram of the plaintext image. This helps prevent attackers from extracting information from the ciphertext images. The histograms of the encrypted images produced by the proposed encryption method are uniform and distinct from the histograms of the plaintext images, as illustrated in Figure 12m–p.

## 6 | CONCLUSION

To address the privacy and security challenges in 5G-enabled healthcare applications while taking the latency issues into consideration, this paper presents a time-efficient encryption scheme that ensures an appropriate level of security for digital images and also decreases computational complexity. The computational complexity is reduced by the use of bit-plane extraction methodology and the DWT. The encryption process only takes into account those frequency bands and bit-planes that contain the highest proportion of the original plaintext image. To resolve the aforementioned issue, a time-efficient encryption algorithm is proposed that provides an adequate level of security. Furthermore, to make the scheme lightweight and to reduce the encryption time, DWT and bit-plane extraction methodologies are incorporated, in which only such frequency band and bit-planes are considered for encryption which contains a maximum percentage of the

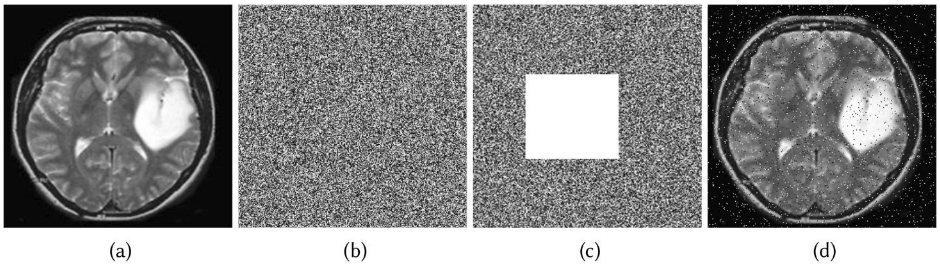


**FIGURE 11** Cropping attack analysis of the proposed scheme: (a) Plaintext image (b) Encrypted image (c) Cropped version of the encrypted image (d) Decrypted of original image from cropped version of the encrypted image.

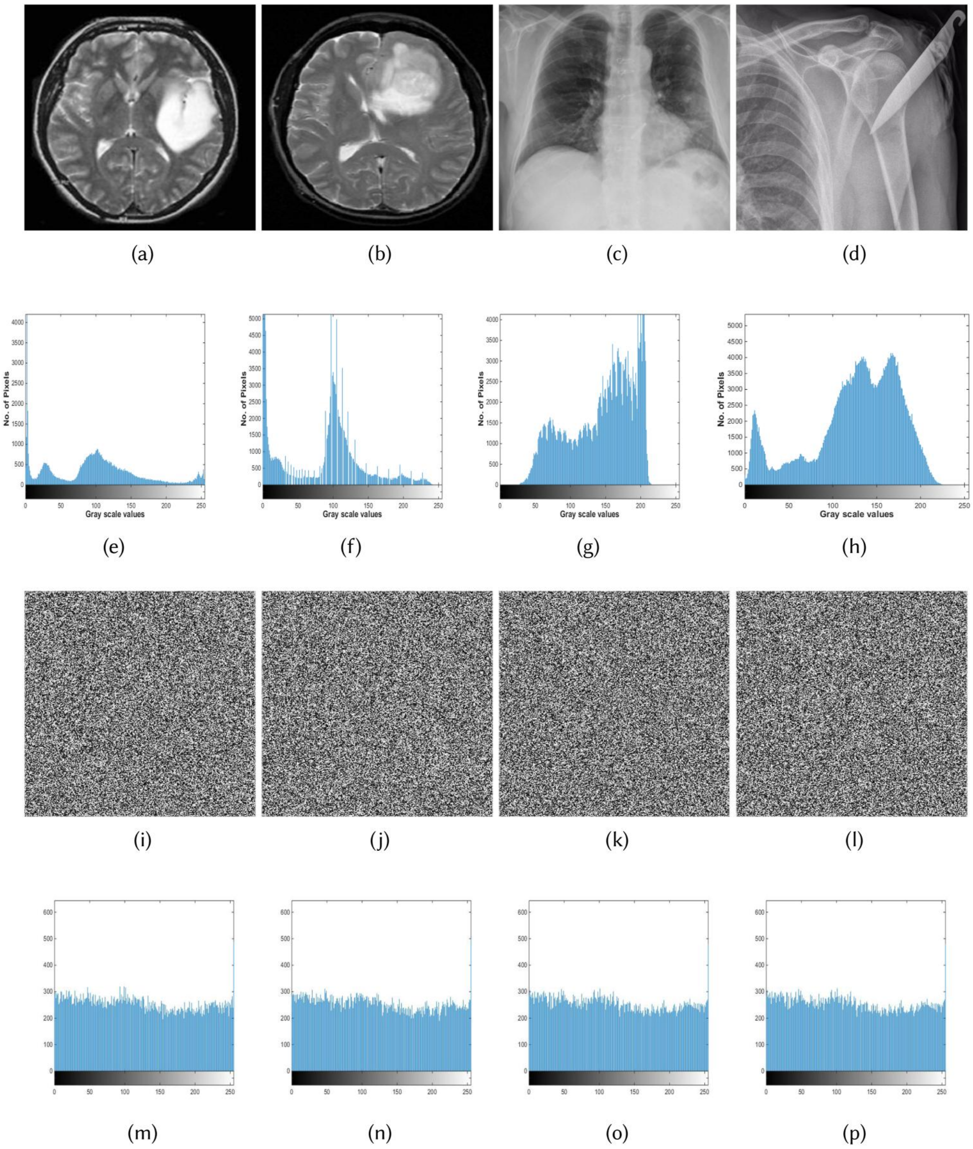


**FIGURE 12** Histogram analysis of plaintext and the corresponding ciphertext images: (a–d) Plaintext images, (e–h) Histograms of plaintext images, (i–l) Ciphertext images (m–p) Histograms of ciphertext images.

amount of plaintext image. Moreover, the proposed encryption scheme can encrypt multiple grayscale images simultaneously, reducing the computational cost by up to 66%. For instance, if an encryption scheme takes 1 s to encrypt one grayscale image of size $M \times N$, it will take 3 s to encrypt three grayscale images. Consequently, the proposed encryption scheme will take 0.33 s to encrypt three images of the same size ($M \times N$).

## 7 | FUTURE WORK

The proposed scheme has not yet been tested on a smartphone. However, the proposed work can be designed for mobile applications in the future. Moreover, the proposed scheme can be extended for audio and video encryption.

### ACKNOWLEDGEMENT

The authors would like to thank Prince Sultan University for their support. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large group Research Project under grant number RGP.2/379/44.

### CONFLICT OF INTEREST STATEMENT

We wish to confirm that there are no known conflicts of interest associated with this publication.

### DATA AVAILABILITY STATEMENT

Data available on request from the authors.

### ORCID

*Jawad Ahmad* https://orcid.org/0000-0001-7495-2248

### REFERENCES

1. Khan, J.S., Ahmad, J.: Chaos based efficient selective image encryption. Multidimens. Syst. Signal. Process. 30(2), 943–961 (2019). 2019
2. Nematzadeh, H., et al.: Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng 110, 24–32 (2018). 2018
3. Kakkad, V., Patel, M., Shah, M.: Biometric authentication and image encryption for image security in cloud framework. Multiscale Multidiscip. Model. Exp. Des. 2(4), 233–248 (2019). 2019
4. Boulila, W., et al.: Securing the classification of covid-19 in chest x-ray images: a privacy-preserving deep learning approach. In: 2022 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pp. 220–225. IEEE (2022)
5. Rashmi, P., Supriya, M.C., Hua, Q.: Enhanced Lorenz-chaotic encryption method for partial medical image encryption and data hiding in big data healthcare. Secur. Commun. Netw. 2022 (2022). 2022
6. Alabaichi, A., Ahmad, F., Mahmod, R.: Security analysis of blowfish algorithm. In: 2013 Second International Conference on Informatics & Applications (ICIA), pp. 12–18. IEEE (2013)
7. Basu, S.: International data encryption algorithm (idea)–a typical illustration. J. Glob. Res. Comput. Sci. 2(7), 116–118 (2011). 2011
8. Daemen, J., Vincent, R.: Reijndael: the advanced encryption standard. Dr. Dobb's J. 26(3), 137–139 (2001). 2001
9. Data Encryption Standard, et al.: Data encryption standard. Fed. Inform. Process. Standards Publ. 112 (1999). 1999
10. Tang, Z., et al.: Multiple-image encryption with bit-plane decomposition and chaotic maps. Opt. Lasers Eng. 80, 1–11 (2016). 2016
11. Ahmad, J., Hwang, S.O.: Chaos-based diffusion for highly autocorrelated data in encryption algorithms. Nonlinear Dyn. 82(4), 1839–1850 (2015). 2015
12. Lakhan, A., et al.: Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. IEEE J. Biomed. Health Inform. 27(2), 664–672 (2022). 2022
13. Li, H., et al.: An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things. IEEE J. Biomed. Health Inform. 26(5), 1949–1960 (2021). 2021
14. Chandra Barik, R., Changder, S.: A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps. Multimed. Tools Appl. 80(7), 10723–10760 (2021). 2021
15. Sheela, S.J., et al.: Cellular neural network-based medical image encryption. SN Comput. Sci. 1(6), 1–11 (2020). 2020
16. Han, B., et al.: Application of robust zero-watermarking scheme based on federated learning for securing the healthcare data. IEEE J. Biomed. Health Inform. (2021). 2021
17. Wang, R., et al.: Privacy-preserving federated learning for internet of medical things under edge computing. IEEE J. Biomed. Health Inform. 27(2), 854–865 (2022). 2022
18. C Dagadu, J., Li, J.-P., Emelia, O.A.: Medical image encryption based on hybrid chaotic DNA diffusion. Wirel. Pers. Commun. 108(1), 591–612 (2019). 2019
19. Liao, X., et al.: An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik-Int. J. Light Electron Opt. 153, 117–134 (2018). 2018
20. Chai, X., et al.: A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput. Appl. 31(1), 219–237 (2019). 2019
21. Ibrahim, S., et al.: Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps. IEEE Access 8(2020), 160433–160449 (2020)
22. Anees, A., Siddiqui, A.M., Ahmed, F.: Chaotic substitution for highly autocorrelated data in encryption algorithm. Commun. Nonlinear Sci. Numer. Simul. 19(9), 3106–3118 (2014). 2014
23. Guesmi, R., Farah, M.A.: A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimed. Tools Appl. 80(2), 1925–1944 (2021). 2021
24. Jiang, N., et al.: Quantum image encryption based on Henon mapping. Int. J. Theor. Phys. 58(3), 979–991 (2019). 2019
25. Ye, G., Huang, X.: An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing 251, 45–53 (2017). 2017
26. Phadikar, S., Sinha, N., Ghosh, R.: Automatic eyeblink artifact removal from EEG signal using wavelet transform with heuristically optimized threshold. IEEE J. Biomed. Health Inform. 25(2), 475–484 (2020). 2020
27. Li, C., Yang, X.: An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. Optik 260(2022), 169042 (2022)
28. Dubey, S.R., Singh, S.K., Singh, R.K.: Local bit-plane decoded pattern: a novel feature descriptor for biomedical image retrieval. IEEE J. Biomed. Health Inform. 20(4), 1139–1147 (2015). 2015
29. Liu, X., Xiao, Di, Liu, C.: Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. Quantum Inform. Process. 19(8), 1–23 (2020). 2020
30. El-Latif, A.A.A., et al.: Efficient chaos-based substitution-box and its application to image encryption. Electronics 10(12), 1392 (2021). 2021
31. Ben Farah, M.A., et al.: A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt. Laser Technol. 121(2020), 105777 (2020)
32. Silva-García, V.M., et al.: Substitution box generation using Chaos: an image encryption application. Appl. Math. Comput. 332, 123–135 (2018). 2018
33. Chen, L., et al.: Chaos in fractional-order discrete neural networks with application to image encryption. Neural Netw. 125(2020), 174–184 (2020)
34. Man, Z., et al.: Double image encryption algorithm based on neural network and chaos. Chaos Solit. Fractals 152(2021), 111318 (2021)

**How to cite this article:** Rehman, M.U., et al.: A novel medical image data protection scheme for smart healthcare system. CAAI Trans. Intell. Technol. 1–16 (2024). https://doi.org/10.1049/cit2.12292