frontiers | Frontiers in Computational Neuroscience

TYPE Original Research
PUBLISHED 06 June 2025
DOI 10.3389/fncom.2025.1591972

OPEN ACCESS

EDITED BY
Saad Arif,
King Faisal University, Saudi Arabia

REVIEWED BY
Farman Ali,
Sungkyunkwan University, Republic of Korea
Zeba Idrees,
University of Alberta, Canada

*CORRESPONDENCE
Abdullah Aziz
✉ abdullah.aziz@umu.se

RECEIVED 11 March 2025
ACCEPTED 14 May 2025
PUBLISHED 06 June 2025

CITATION
Asiri F, Al Malwi W, Zhukabayeva T, Nafea I, Aziz A, Gazem NA and Qayyum A (2025) Enhancing medical image privacy in IoT with bit-plane level encryption using chaotic map. *Front. Comput. Neurosci.* 19:1591972. doi: 10.3389/fncom.2025.1591972

Enhancing medical image privacy in IoT with bit-plane level encryption using chaotic map

Fatima Asiri[1], Wajdan Al Malwi[1], Tamara Zhukabayeva[2], Ibtehal Nafea[3], Abdullah Aziz[4]*, Nadhmi A. Gazem[5] and Abdullah Qayyum[6]

[1]Informatics and Computer Systems Department, College of Computer Science, King Khalid University, Abha, Saudi Arabia, [2]Department of Information Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, [3]College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia, [4]High Performance Computing Centre North, Umeå University, Umeå, Västerbotten, Sweden, [5]Department of Information Systems, College of Business Administration-Yanbu, Taibah University, Medina, Saudi Arabia, [6]6G Lab, School of Engineering and Informatics University of Sussex, Brighton, United Kingdom

Introduction: Preserving privacy is a critical concern in medical imaging, especially in resource limited settings like smart devices connected to the IoT. To address this, a novel encryption method for medical images that operates at the bit plane level, tailored for IoT environments, is developed.

Methods: The approach initializes by processing the original image through the Secure Hash Algorithm (SHA) to derive the initial conditions for the Chen chaotic map. Using the Chen chaotic system, three random number vectors are generated. The first two vectors are employed to shuffle each bit plane of the plaintext image, rearranging rows and columns. The third vector is used to create a random matrix, which further diffuses the permuted bit planes. Finally, the bit planes are combined to produce the ciphertext image. For further security enhancement, this ciphertext is embedded into a carrier image, resulting in a visually secured output.

Results: To evaluate the effectiveness of our algorithm, various tests are conducted, including correlation coefficient analysis ($C.C$ $<$ or negative), histogram analysis, key space [$(10^{90})^8$] and sensitivity assessments, entropy evaluation [$E(S) > 7.98$], and occlusion analysis.

Conclusion: Extensive evaluations have proven that the designed scheme exhibits a high degree of resilience to attacks, making it particularly suitable for small IoT devices with limited processing power and memory.

KEYWORDS

image encryption, Chen chaotic map, chaos, meaningful encryption, bit-level encryption, IoT

1 Introduction

The Internet of Things (IoT) connects devices and objects via the Internet, whether wirelessly or wired. In recent years, the concept has become increasingly popular as it is used for various purposes, including business development, transportation, education, and communication. The hyper-connectivity created by the IoTs enables individuals and organizations to communicate seamlessly from a distance (Porras et al., 2018). IoT has been widely embraced in a wide range of industries, including e-health, manufacturing, smart cities, agribusiness, and home automation. According to Cisco, Internet-connected gadgets will number approximately 500 billion by 2030 (Aman et al., 2020). As IoT advances exponentially, medical imaging and data have become more widely used, and are therefore need to be secured before being shared.

Medical images have become increasingly important in diagnosing and treating illnesses. The visuals are used directly by doctors during the evaluation and therapy of patients (Ismail et al., 2018). For medical applications, securing the transmission and storage of medical images has become increasingly important due to their containment of private information (Ye and Huang, 2015; Dridi et al., 2016; Al-Haj et al., 2015; Cao et al., 2017; Khan et al., 2018; Hu et al., 2024; Chu et al., 2024; Belazi et al., 2019). A number of academics have therefore focused on developing methods to secure images in IoT applications. The authors in Ye and Huang (2015) utilized logistic and Arnold chaotic maps to design an autoblocking and Electrocardiography (ECG) signal-based medical image encryption scheme. ECG signals and the Wolf algorithm calculates initial conditions for the chaotic system. A key characteristic of this cryptoarchitecture is that it performs autoblocking diffusion only during the encryption phase of the process, in contrast to traditional cryptoarchitectures. A new chaos and neural network-based medical image encryption scheme has been presented in Dridi et al. (2016). Plaintext image pixels are XORed with a generated key. The weight and bias values for neural networks have been computed using the Logistic map. By using this technique, medical images can be made more secure with a simpler algorithm than current ones. Using Strong cryptographic functions with internal symmetric keys and hash codes, the author designed an encryption scheme for medical images that ensures confidentiality, authenticity, and integrity (Al-Haj et al., 2015). With the whirlpool hash function and Galois counter mode, advanced encryption standards are used to secure confidentiality and authenticity, while digital signature algorithms employ elliptic curves to secure integrity and authenticity. The edge map-based medical encryption scheme has been presented in Cao et al. (2017). It consists of three main steps: (a) extraction of bit planes, (b) generating random numbers, and (c) permutations. The source image can be any type of image and distinct edge maps can be produced by varying edge detection approaches and thresholds, depending on the source image type. An Intertwining Logistic map and Deoxyribonucleic acid (DNA) are utilized by Khan et al. to protect medical images (Khan et al., 2018). A DNA sequence is passed through SHA-512 in order to calculate the chaotic system's initial condition. Plaintext pixel correlations are broken down through shuffling. In addition to XORing, an affine transformation is also applied to diffuse the shuffled pixels. A two-round medical encryption scheme is designed by Belazi et al. by combining chaos and DNA (Belazi et al., 2019). During each round, six steps are performed, namely block permutation, pixel substituting, DNA encoding, bit substitution, DNA decoding, and bit diffusion.

As Internet-related technologies continue to grow exponentially, new technologies, energy, or modifications are added daily. Applications and systems that use the Internet of Things benefit greatly from the recent advancements in wireless technology from 1G to 5G (Hasan et al., 2021). In recent years, high-quality medical care has become increasingly important as a result of population growth, urbanization, and the COVID-19 pandemic (Trujillo-Toledo et al., 2023). In medical diagnostics, X-rays, Computer Tomography Scans (CT scans), nuclear medicine imaging, and ultrasounds are modern imaging techniques. Thus, these high-resolution diagnostic images need to be secured before being exchanged. Recently, cyber attacks could make healthy patients appear sick and vice versa. Therefore, cyber-security threats will increase alarmingly in the area of medical image communication. It is therefore increasingly important to have fast and secure cyber-security systems regarding the diagnosis of medical images (Kester et al., 2015). The Internet of Medical Things (IoMT) can provide many advantages to hospitals and healthcare organizations. However, they need to ensure that the right policies and protocols are in place to tackle the security challenges posed by IoMT. Researchers are curious about the potential security and privacy issues associated with this concept, particularly when bandwidth and frequency are high. Therefore, it is essential to design a robust medical image encryption scheme to guarantee the safe and trustworthy transmission and receipt of patients' symptomatic data through IoT. Double permutation techniques are used in Hasan et al. (2021) to design a lightweight, efficient encryption algorithm to protect healthcare images. In this method, plaintext images are broken down into blocks and encrypted. A chaotic encryption technique, based on the Message Queuing Telemetry Transport (MQTT) protocol, is proposed in this research for enhancing security and secrecy when transmitting medical images over the Healthcare Internet of Things (H-IoT) network (Trujillo-Toledo et al., 2023). Initially, chaotic maps are enhanced and applied to encrypt plaintext pixels through diffusion. The designed scheme efficiency is confirmed via a number of tests. The designed embedded medical cryptosystems transmit real-time medical images over the Internet and WiFi, thus enhancing real-time medical image security. Using multiple chaotic maps, the authors propose Multiple Map Chaos Based Image Encryption (MMCBIE) scheme, a novel method that encrypts images in the IoT environment (Jain et al., 2024). Unlike existing schemes, MMCBIE combines multiple chaotic maps, like Henon and 2D Logistic chaotic maps in a unique combination. According to security assessments and cryptanalysis, MMCBIE possesses high-level security properties, making it a superior method of image encryption. Hanchate and Anandan (2024) presented a hybrid scheme that combines Adaptive Elliptic Curve Cryptography (AECC) and Logistic mapping to encrypt medical images for the IoT. As a first step, the image is encrypted using the AECC technique, then again encrypted using the logistic map-based DNA sequence algorithm for greater security. The diffused DNA matrix is then decoded to produce the cipher image. The plain image determines the rules for encoding and decoding DNA as well as the key matrix. Liu et al. (2024) utilize compressive sensing (CS) and chaotic systems to design an encryption scheme for IoT scenarios to ensure security and efficiency. A chaotic laser system generates Masuemet matrices with complex phase space. The measurement matrices are further enhanced through the use of cyclic matrix methods. The image reconstruction quality is further improved using segmented linear thresholding. Further, large images are compressed block-wise in order to reduce storage space and improve reconstruction efficiency. The authors in Nadhan and Jacob (2024) investigated how a cryptography-based network might be able to encode medical images, as well as how deep learning could be used to ensure that the images are transmitted safely. Various image representations have been mapped using the ResNet-50 architecture. As a result of the extensive empirical setup and the security analysis, the suggested method is likely to provide unprecedented levels of

security. An IWT-based DNA encoding scheme is proposed to encrypt medical images within the Healthcare IoT (Lai and Hua, 2025). Random sequences were generated using a 3D hyperchaotic map. In addition to IWT, a novel diffusion algorithm masks critical information by generating approximation components. Bit-level permutations further enhance encryption complexity. The scheme further uses the DNA shuffle technique and encrypts the permuted images using a DNA-encoding technique to enhance security.

Most traditional image encryption algorithms convert plain images into noise-like ciphers, making them easily detectable and vulnerable to attack during transmission or storage. Visual security should be considered when designing an image encryption method to avoid hackers' attention. Therefore, to avoid the eavesdropper's attention, meaningful image encryption algorithms must be developed that may generate visually meaningful ciphertext images. Image encryption algorithms that provide a visual sense of meaning have attracted considerable research attention (Khan et al., 2024, 2020; Gan et al., 2024; Sathananthavathi et al., 2024; Zhang et al., 2024). A bit plane image encryption scheme was designed by Khan et al. (2024) using hash function and chaos theory. A SHA-512 hash algorithm is used to compute the key for the chaotic map. The chaotic random vectors are used to shuffle the plaintext image pixels row- and column-wise, while the random matrix is used for XOR-based diffusion. By embedding the noise-like ciphered text within a host image, a visually secure ciphertext image has been generated. The authors in Khan et al. (2020), presented a chaotic visual selective image encryption scheme. The key for the scheme has been derived from the DNA and plaintext image. The system keyspace is increased by using three different chaotic 1D maps. The original image is divided into blocks of varying sizes. Blocks with correlation coefficients above a predefined threshold are XORed with random matrices. The diffused blocks are then permuted to break the correlation between pixel values. As a final step, the ciphertext is encapsulated in a carrier image to create a visually secure ciphertext image.

Contribution

- The enhanced medical image encryption scheme has confusion and diffusion characteristics, making it ideal for the IoT environment.
- This scheme resists classical attacks due to its reliance on plaintext images as keys.
- To avoid attackers' attention, ciphered images are embedded in carrier images to produce visually secure images.

The remaining article is organized as follows: Section 2 discusses the preliminaries; Section 3 outlines the proposed methodology; the result analysis of the proposed work is provided in Section 4. Conclusion is provided in Section 5.

2 Preliminaries

2.1 Chaotic Chen system

Using simple state feedback, Chen developed a new 3D chaotic system in 1999 [1]. Similarly to the Lorenz system, Chen's second and third equations contain cross-product terms. From a topological point of view, the Lorenz and Chen systems have different structures. Mathematically, the system can be written as Qi et al. (2005):

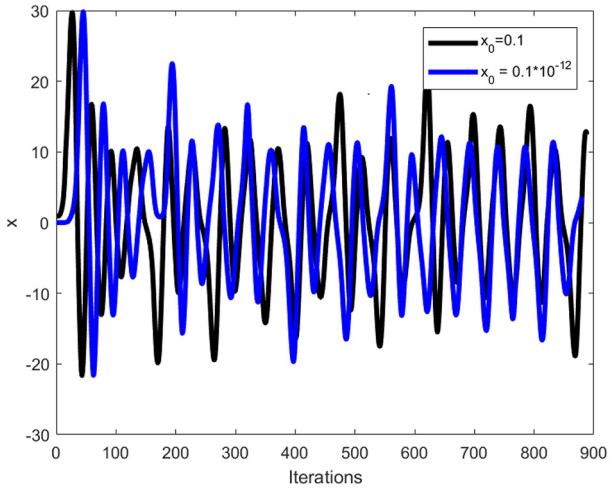

FIGURE 1
Sensitivity plot of chaotic Chen system.

$$\begin{aligned} \dot{x} &= a * (y - x), \\ \dot{y} &= ((c - a) * x) + (c * y) - (x * z), \\ \dot{z} &= (x * y) - (b * z). \end{aligned} \tag{1}$$

where x, y, and z are the variables indicating the state of the system, and a, b, and c are the parameters. It has been proven that the Chen system has chaotic behavior for parameter values being $\alpha > 0.82$ and $a = 35, b = 3$, and $c = 28$. In the proposed scheme, the random numbers will be computed using the $\alpha = 0.9$ value. In order to illustrate Chen system sensitivity, the chaotic system is iterated twice with $x_0 = 0.01$ and $x_0 = 0.01 \times 10^{-12}$. Thus, one can confirms that both the sets of random numbers in Figure 1 are different. Further, Figure 2 shows three sets of 8,000 random numbers generated through the Chen chaotic system. Therefore, one can conclude that the chaotic system is extremely sensitive and produces different random numbers with small changes in the initial condition or control parameter.

2.2 SHA-512

In 2002, the National Security Agency (NSA) developed a cryptographic hashing algorithm named Secure Hash Algorithm 2 (SHA-2) (Wang et al., 2021). Compared to its predecessors SHA-0 and SHA-1, SHA-2 provides a more robust solution. SHA-512 is the most secure and efficient hash function in the SHA-2 family (Bhonge et al., 2020). Based on an arbitrary message length, it computes a 512-bit hash value by splitting the data into blocks of 1024 bits and passing the data through the module, consisting of 80 rounds. In our proposed scheme, SHA-512 is used to generate eight 512-bit hash values for eight plaintext bit planes, respectively. The

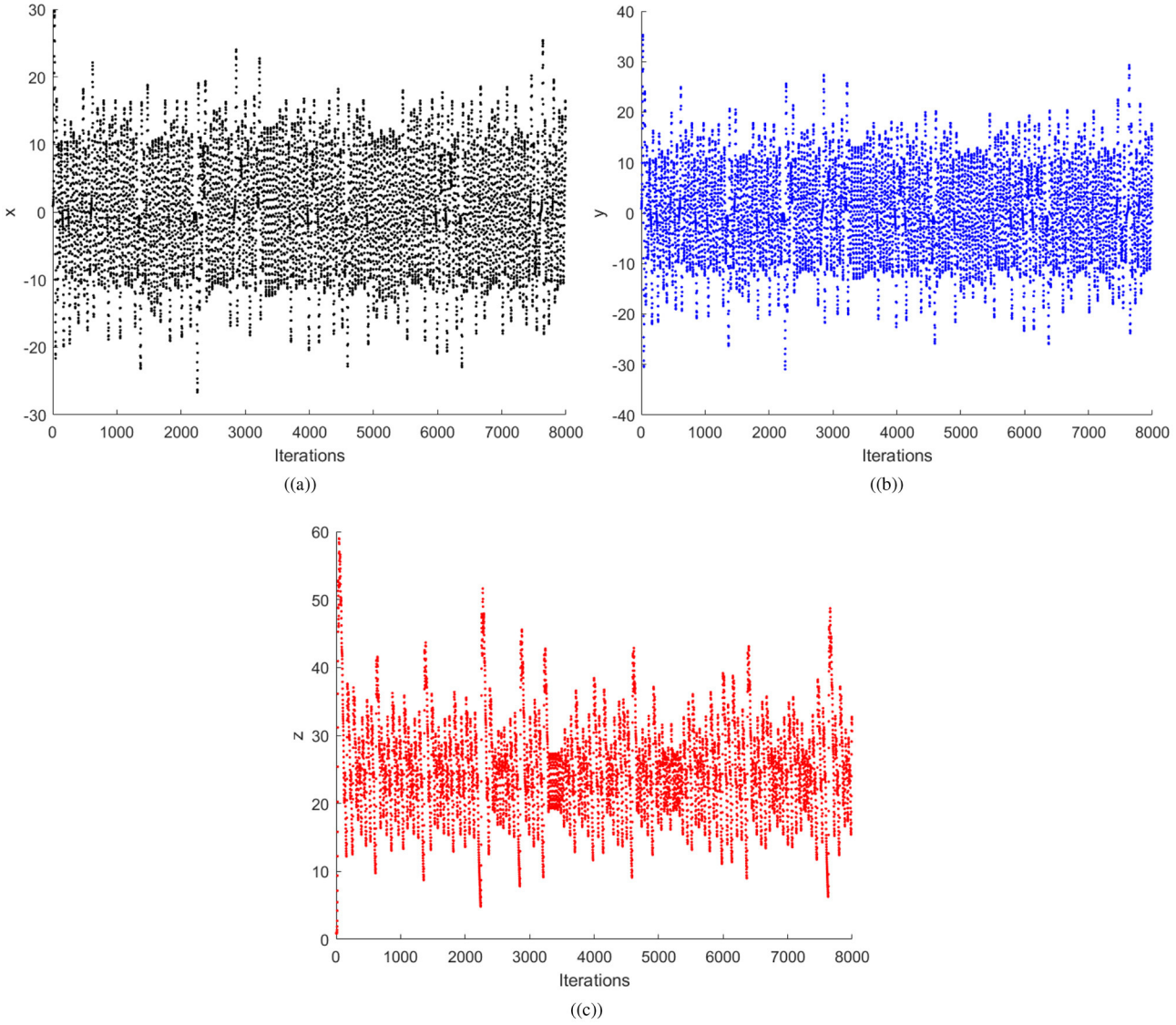

FIGURE 2
Random number plots: **(a)** x vector, **(b)** y vector, and **(c)** z vector.

hash values are used to generate the initial conditions of the chaotic system.

3 Proposed methodology

To divert the attention of an attacker, visually secure encryption facilitates the transfer of private information over an insecure channel. This process embeds the ciphertext image into a carrier or host image to produce visually secure ciphertext images. Figure 3 illustrates the general workflow of an image encryption scheme while Figure 4 demonstrates the step-by-step flow chart of the proposed meaningful privacy preservation of medical images in IoT environments. An end-to-end encryption method has been developed that enables medical images to be transmitted over the Internet using any H-IoT device with enhanced security and confidentiality. The proposed scheme is comprised of the following steps:

Step: 1 Let the original plaintext medical image with dimensions $m \times n$ can be represented as M and its constituent bit planes can be represented as:

$$M = [M_1, M_2, M_3, ..., M_8]. \tag{2}$$

Step: 2 To determine the initial conditions for the Chen chaotic system and to ensure the integrity and non-repudiation of the image data, each of these planes is cryptographically hashed utilizing SHA-512.

$$H_1 = SHA - 512(M_1). \tag{3}$$

Step: 3 For numerical interpretation purposes, the computed H_1 value is converted to a decimal value.

$$N = bi2de(H_1). \tag{4}$$

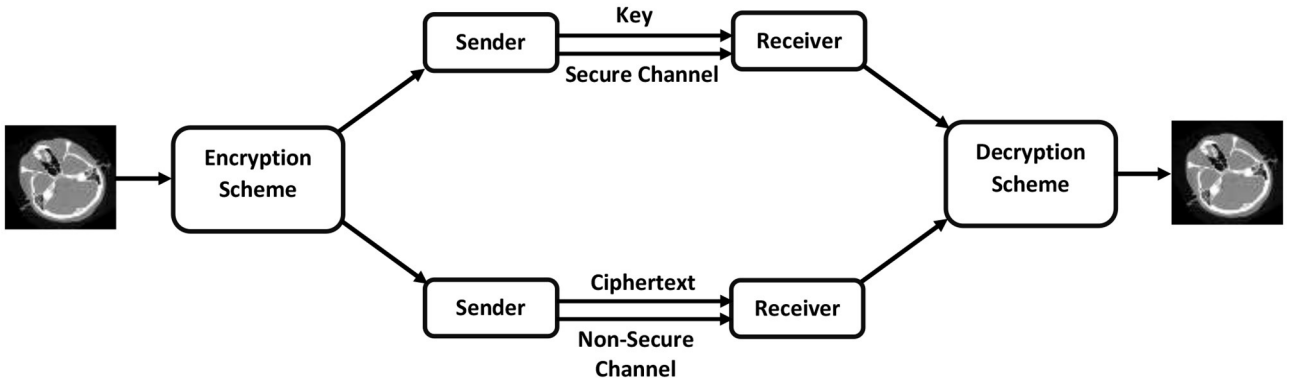

FIGURE 3
General encryption methodology.

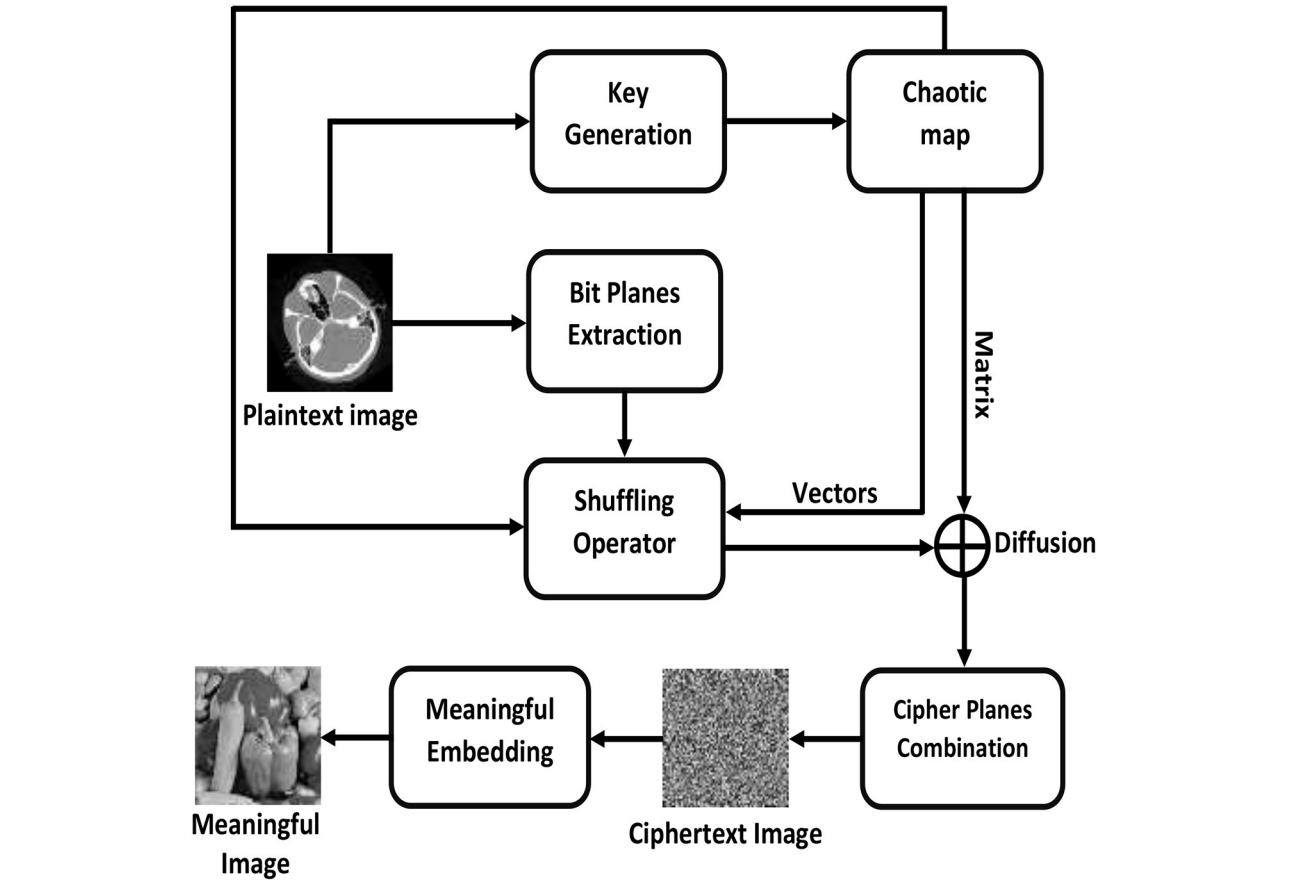

FIGURE 4
A detailed step-wise flowchart of the proposed scheme.

Step: 4 Now, the initial conditions can be calculated as follows:

$$x_0, y_0 \, and \, z_0 = \frac{N}{2^{48}}. \tag{5}$$

Step: 5 The chaotic Chen system is iterated to generate three random vectors x, y, and z.

Step: 6 For each generated random vector x, y, and z, the *Mod*256 is applied to bring the values within the range of 0 and 255.

$$x, y \, and \, z = \mathrm{mod}\left((x, y, \, and \, z) \times 10^{14}, 256\right). \tag{6}$$

Step: 7 The vectors x and y are utilized to permute the plaintext medical image M row- and column-wise, respectively.

$$R_M = x(M),$$

$$C_M = y(R_M). \tag{7}$$

Step: 8 The vector z is rearranged in a matrix and XORed bitwise with the permuted image to generate the final medical bit-plane ciphertext.

$$C_M = z \oplus C_M. \tag{8}$$

Step: 9 Steps 2 through 8 must be repeated eight times to encrypt each layer.

Step: 10 Combine all ciphertext planes to produce the final ciphertext or encrypted medical image.

$$C = [C_{M1}, C_{M2}, C_{M3}, ..., C_{M8}]. \tag{9}$$

Step: 11 The carrier image C_C is passed through the Lifting Wavelet Transformation (LWT).

$$[LL, LH, HL, HH] = LWT(C_C) \tag{10}$$

Step: 12 The ciphertext image C is divided into 4 Most Significant Bits (MSBs) and 4 Least Significant Bits (LSBs). Now, the HL and HH blocks of C_C are replaced by the MSBs and LSBs. Finally, the Inverse Lifting Wavelet Transformation (ILWT) was used to generate a visually meaningful medical image V_M. As the final visually meaningful medical image V_M contains values greater than 255 and less than 0, it is scaled by a min-max normalization function to keep them between 0 and 255.

$$V_M = ILWT[LL, LH, MSBs, LSBs] \tag{11}$$

Decryption can be accomplished by reversing all of the above steps in reverse order.

4 Results

This section presents simulations to illustrate the effectiveness and robustness of the proposed scheme. Our analysis in this section demonstrates that the IoT encryption scheme developed for medical images is robust against different security attacks. Figure 5 shows the encryption outcomes of the designed scheme for cthead and chest images of size 128 × 128. The ciphered images in Figures 5c, g are noise-like images, so they are encapsulated inside a carrier image (Pepper image of size 256 × 256) to generate a visually secure medical image. Further, correlation analyses, histogram analyses, entropy analyses, key sensitivity, key space analyses, robustness analyses, etc, are performed to demonstrate the strength of the developed medical image encryption scheme for IoT against statistical attacks, brute force attacks, noise attacks, and classical attacks.

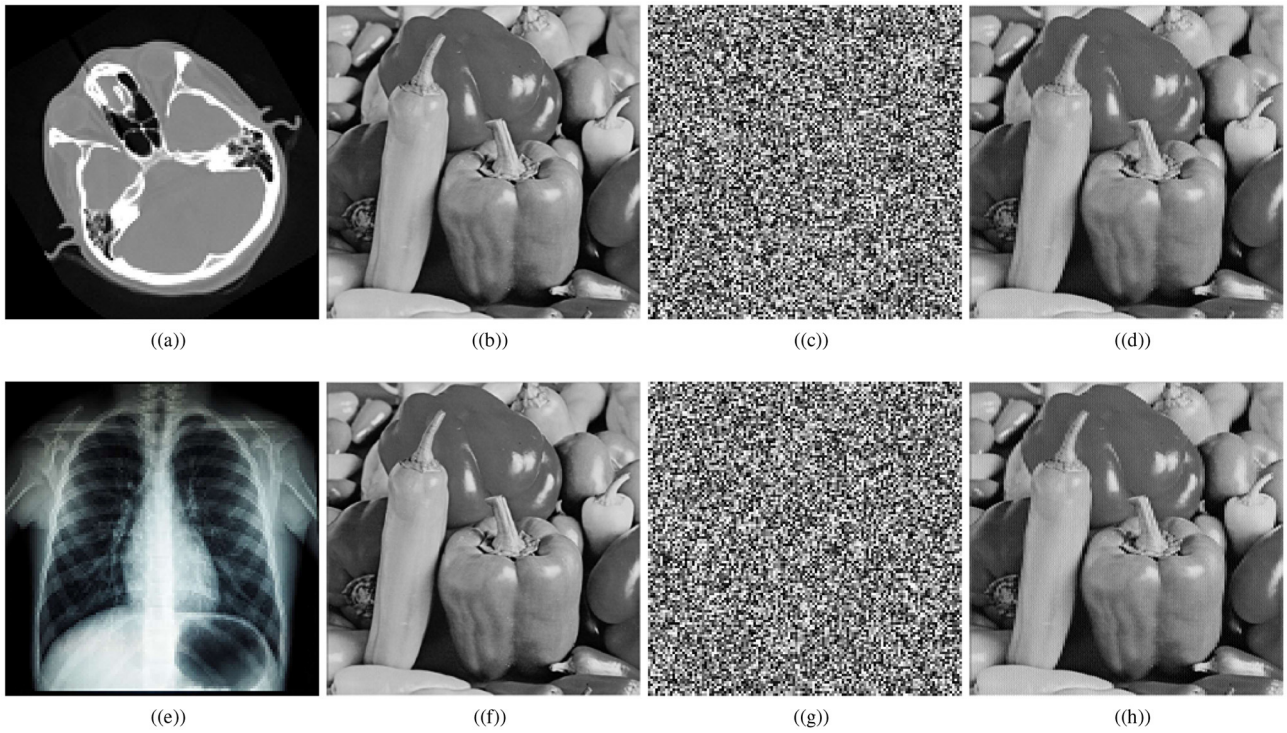

FIGURE 5
Encryption results: **(a)** plaintext cthead image, **(b)** carrier plaintext image, **(c)** ciphertext cthead image, **(d)** visually secure image, **(e)** plaintext chest image, **(f)** carrier plaintext image, **(g)** ciphertext chest image, **(h)** visually secure image.

4.1 Correlation analysis

Correlation analysis quantifies the relationship between image pixel values. Original plaintext medical images show a close association between neighboring pixels. An encrypted image is secured against pixel relation analysis attacks or statistical attacks when effective cryptographic techniques are applied to reduce the relationship between pixels. A ciphertext image with a lower correlation between adjacent pixels shows a better cryptographic technique. Mathematically, the correlation coefficient can be calculated as follows (Khan and Ahmad, 2019):

$$C.C(x,y) = \frac{\frac{1}{N}\sum_{n=1}^{N}(x_n - E(x))(y_n - E(y))}{\sigma_x \times \sigma_y} \tag{12}$$

where

$$\sigma_x = \sqrt{Var(x)}$$

$$\sigma_y = \sqrt{Var(y)}$$

$$Var(x) = \frac{1}{N}\sum_{n=1}^{N}(x_n - E(x))^2$$

$$Var(y) = \frac{1}{N}\sum_{n=1}^{N}(y_n - E(y))^2$$

The variables N indicate the total number of pixels while Var, σ, and E calculate the variance, standard deviation, and expected operator, respectively. Table 1 summarizes the computed correlation coefficient values for the proposed medical image encryption scheme. Almost all the encrypted images have a $C.C$ value of zero or less than 0. Meanwhile, the carrier or host image and the visually secure image have $C.C$ values near 1. Thus, embedding the ciphertext medical image does not significantly alter the carrier image. Figures 6a–c illustrates the 5,000 adjacent pixels correlation distribution of the original plaintext cthead medical image in three distinct directions, i.e., horizontal (h), vertical (v), and diagonal (d). Figures 6d–f shows the 5,000 adjacent pixels correlation distribution of the corresponding ciphertext image. Therefore, it can be concluded from Figures 6a–c that neighboring pixels are closely associated in the original plaintext medical image. Furthermore, Figures 6d–f confirms that this association breaks down within the ciphered image's pixels, and the correlation among the pixels is totally different. Additionally, Figure 7 shows a strong association between neighbors pixels in the carrier image and the visually secured image, indicating that the visually secured image's pixels are not significantly changed.

4.2 Histogram analysis

Image histograms are statistical plots, plotting the intensity of pixels against the pixel count in a digital image. Mathematically, it can be computed as follows (Singh and Kumar, 2025).

$$H(x_i) = m_i \tag{13}$$

where m_i represents the multiplicity of x_i intensity number. Histogram analysis helps to determine whether pixel intensities are distributed evenly throughout the encryption process. An encryption scheme's robustness against statistical attack can be assessed by ensuring that the encrypted image's histogram is uniform, making it impossible to use statistical analysis to guess the original image's structure (Khan and Ahmad, 2019). Figure 8 shows the histograms of the original and cipher images. Figure 8 confirms the non-uniformity of the histograms for the original cthead and chest images; that is, some pixel intensities may be dominant depending on the contents of the image. In contrast, the cipher images' histograms are uniformly distributed. As a result, the encryption process scrambles pixel values such that no feature of the plaintext image can be identified. Because of the histogram's uniformity, the proposed medical image encryption for IoT is

TABLE 1 Computed correlation coefficient values.

Image	Direction	Plaintext	Ciphertext	Carrier	Visualy secure
Cthead	h	0.9480	0.0097	0.9472	0.9343
	v	0.9577	-0.0062	0.9594	0.9585
	d	0.9224	-0.0499	0.9297	0.9227
Chest	h	0.9768	-0.0384	0.9472	0.9368
	v	0.9628	–0.0258	0.9594	0.9368
	d	0.9340	–0.0380	0.9297	0.9055
Medani et al. (2025)	h	0.9173	–0.0598	-	-
	v	0.8868	0.0386	-	-
	d	0.7851	0.0239	-	-
Kumar and Sharma (2024)	h	0.7586	–0.0075	-	-
	v	0.8665	–0.0071	-	-
	d	0.7261	0.0041	-	-

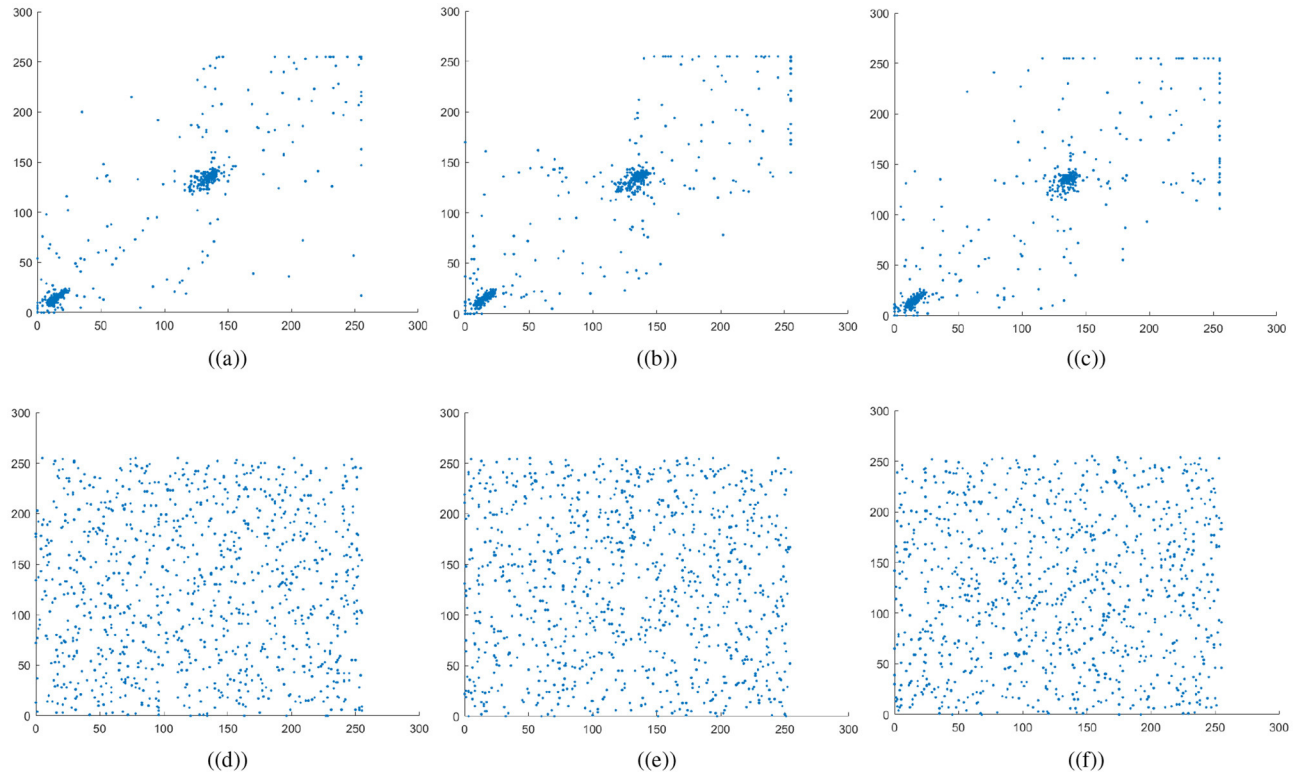

FIGURE 6
Correlation plots for cthead image: **(a–c)** horizontal direction, vertical direction, and diagonal direction plots for plaintext image, **(d–f)** horizontal direction, vertical direction, and diagonal direction plots for encrypted image.

highly resistant to statistical attacks. Histograms of carrier images and visually secured images appear to be nearly identical. Thus, the attacker will not be able to determine that the carrier image is embedded with an encrypted image, as the embedding is not producing significant changes in the host image.

4.3 Key space

In an encryption algorithm, key space refers to all possible secret keys and different parameters. The authors in Alvarez and Li (2006) illustrate how key space size influences the strength of image ciphering techniques. It is essential that the key space be sufficiently large and must exceed 2^{100} to withstand brute force attacks. The proposed meaningful privacy preserving of medical images in IoT environment utilizes the Chen chaotic system, with state variables x, y, and z and control parameters a, b, and c. Each of these parameters has a floating precision of 10^{15}. Further, the map is iterated 8 times for each bit plane. Therefore, the key space of the designed scheme can be computed as follows:

$$K = (10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15})^8$$

$$K = (10^{90})^8 >> 2^{100} \tag{14}$$

Furthermore, the key space computed in Kanwal et al. (2024) and Medani et al. (2025) is 2^{282} and 2^{598}, respectively. Thus, one can conclude that the key space of the presented medical image encryption scheme is sufficiently large to resist a brute force attack significantly.

4.4 Key sensitivity

A good image encryption technique should be able to detect subtle changes in secret keys and parameters, resulting in decoded data that is different from plain image data. The proposed medial image encryption is extremely sensitive to the control parameters and initial conditions. Let's make a small change of 10^{-12} in one of the initial conditions or the control parameters, i.e., x_0 of the Chen chaotic system. As a result, the chaotic system will generate different random numbers. Figure 1 shows the different number generation for a small modification in the initial conditions. Figure 9 illustrates the resultant images after decrypting the ciphertext cthead image with the same and modified keys. A differential image of the two resultant images is shown in Figure 9c. A small change to the initial conditions or control parameters of the Chen chaotic system will fail the decryption process, resulting in a completely different image for the attacker. The differential image demonstrates that both resultant images are different and lack any recognizable information related to the plaintext cthead image. It can therefore be concluded that the proposed meaningful medical image encryption scheme is exceptionally sensitive to even minor changes in the chaotic system control parameters.

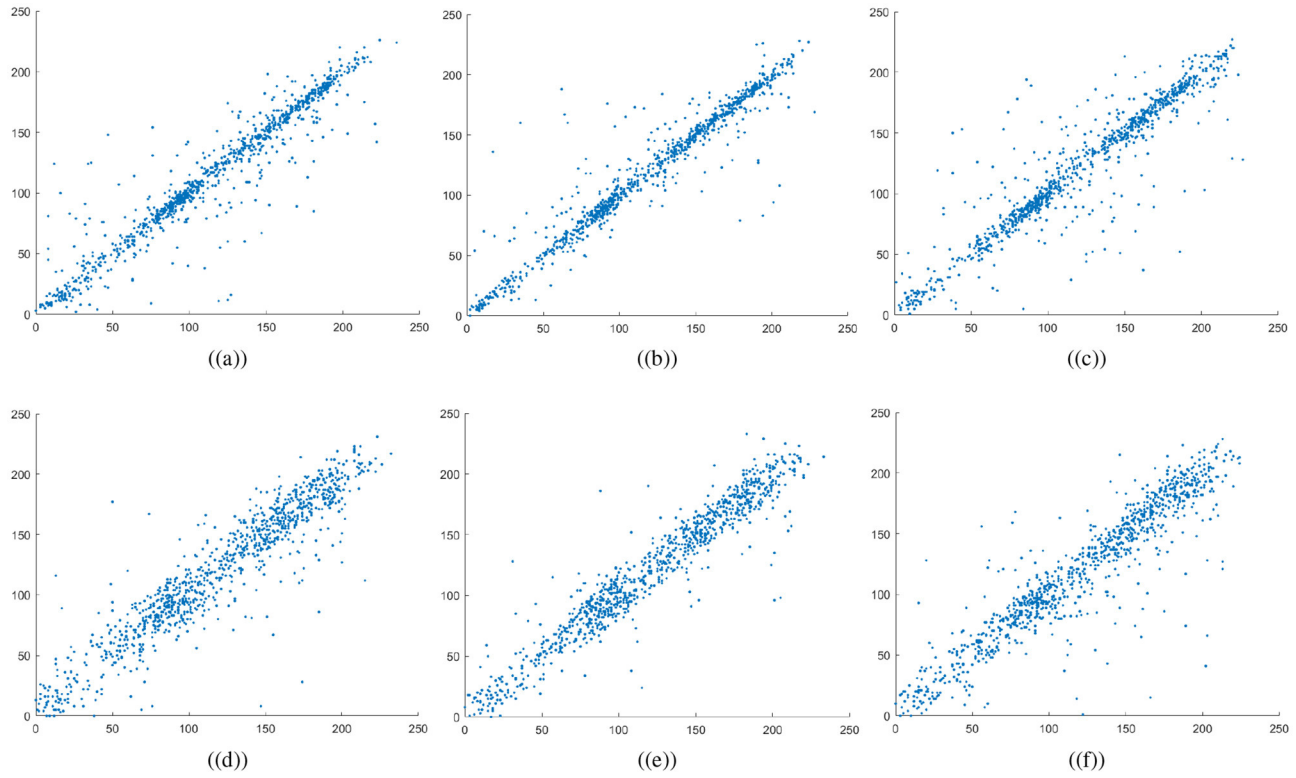

FIGURE 7
Correlation plots for carrier image: first row are horizontal direction, vertical direction, and diagonal direction plots for plaintext carrier image, while the second row are horizontal direction, vertical direction, and diagonal direction plots for encrypted image.

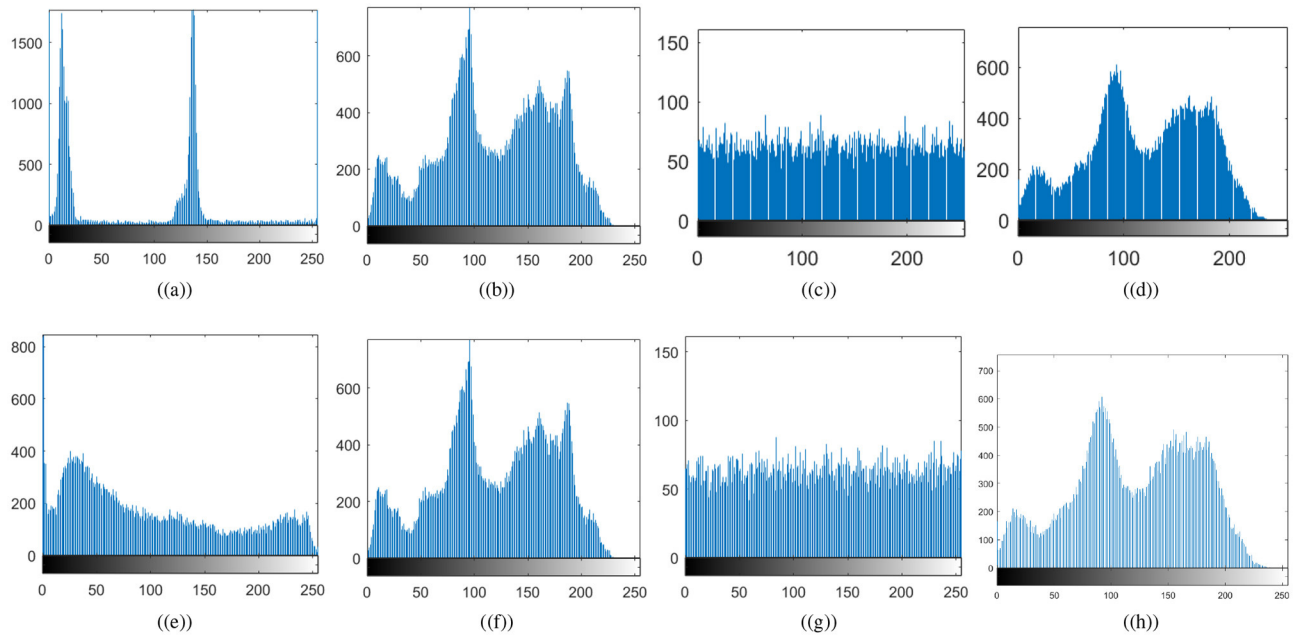

FIGURE 8
Histogram results: **(a)** plaintext cthead image, **(b)** carrier plaintext image, **(c)** ciphertext cthead image, **(d)** visually secure image, **(e)** plaintext chest image, **(f)** carrier plaintext image, **(g)** ciphertext chest image, **(h)** visually secure image.

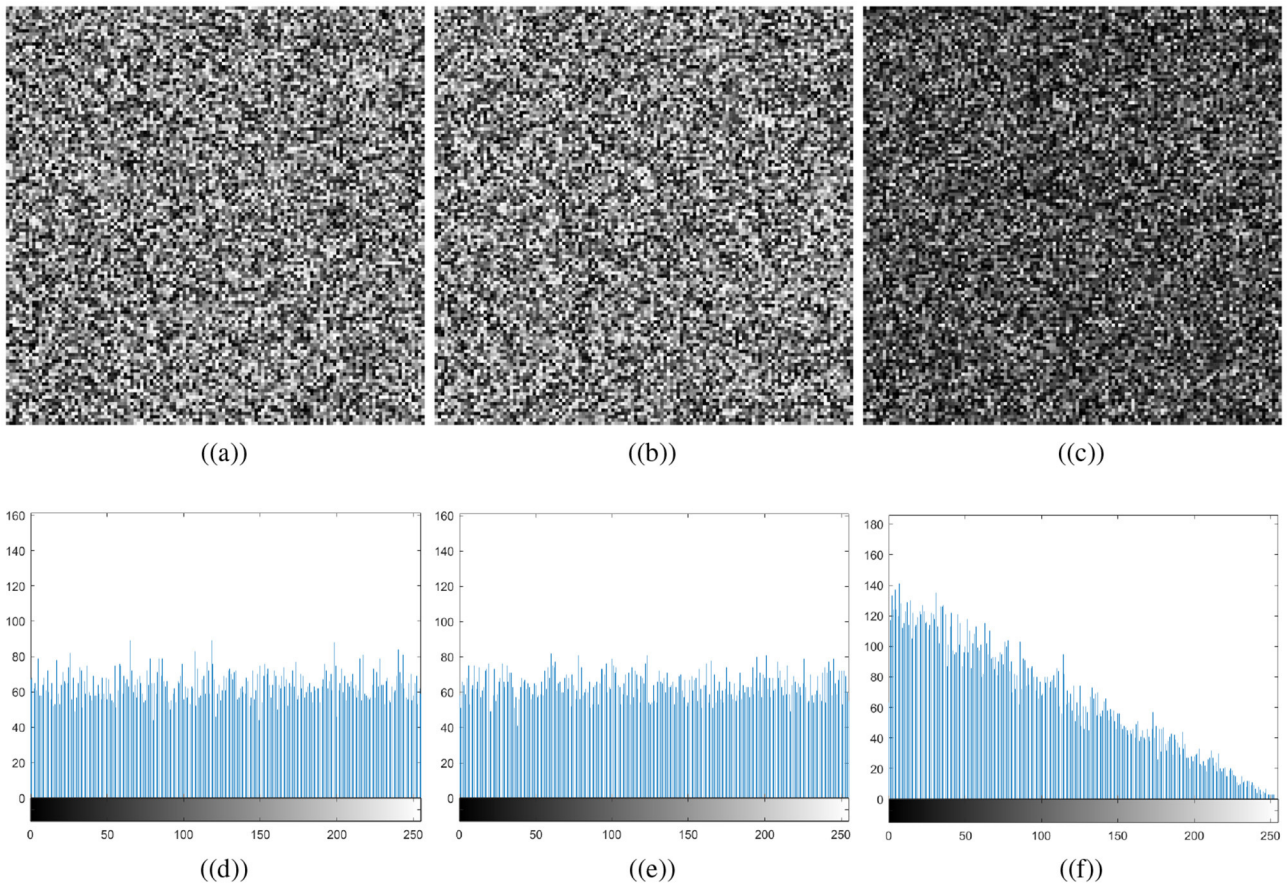

FIGURE 9
Key sensitivity plots: **(a)** original key, **(b)** modified key, **(c)** differential image, and **(d–f)** are the corresponding histograms.

4.5 Entropy analysis

Entropy analysis is usually used to assess image encryption's robustness against entropy attacks. Mathematically, entropy of a data source can be computed as follows (Singh and Kumar, 2025):

$$E(S) = \sum_{k=0}^{256-1} (\frac{1}{256}) log_2(\frac{1}{\frac{1}{256}}) \quad (15)$$

To resist the entropy attack, the entropy value of the encrypted images should be close to 8. Table 2 summarizes the computed entropy values for the proposed medical image encryption scheme. Thus, one can confirm that the entropy value of the ciphertext medical image is approximately equal to 8. The designed technique is robust against entropy attacks without exposing sensitive information.

TABLE 2 Computed entropy values.

Image	Plaintext	Ciphertext	Carrier	Visualy secure
Cthead	5.6763	7.9987	7.6110	7.6485
Chest	7.4040	7.9982	7.6110	7.6498
Medani et al. (2025)	7.6414	7.9998	-	-
Kumar and Sharma (2024)	7.3579	7.9987	-	-

TABLE 3 Number of pixels change rate and unified average change intensity computed values.

Image	NPCR	UACI
Cthead	99.6755%	33.5105%
Chest	99.6867%	33.5241%
Medani et al. (2025)	99.6653%	33.5328%
Kumar and Sharma (2024)	99.5800%	33.1800%

4.6 Differential attack analysis

To measure the effectiveness and reliability of image encryption algorithms against differential attacks, it is important to determine the Number of Pixels Change Rate (NPCR) as well as the Unified Average Change Intensity (UACI). These two matrices can be

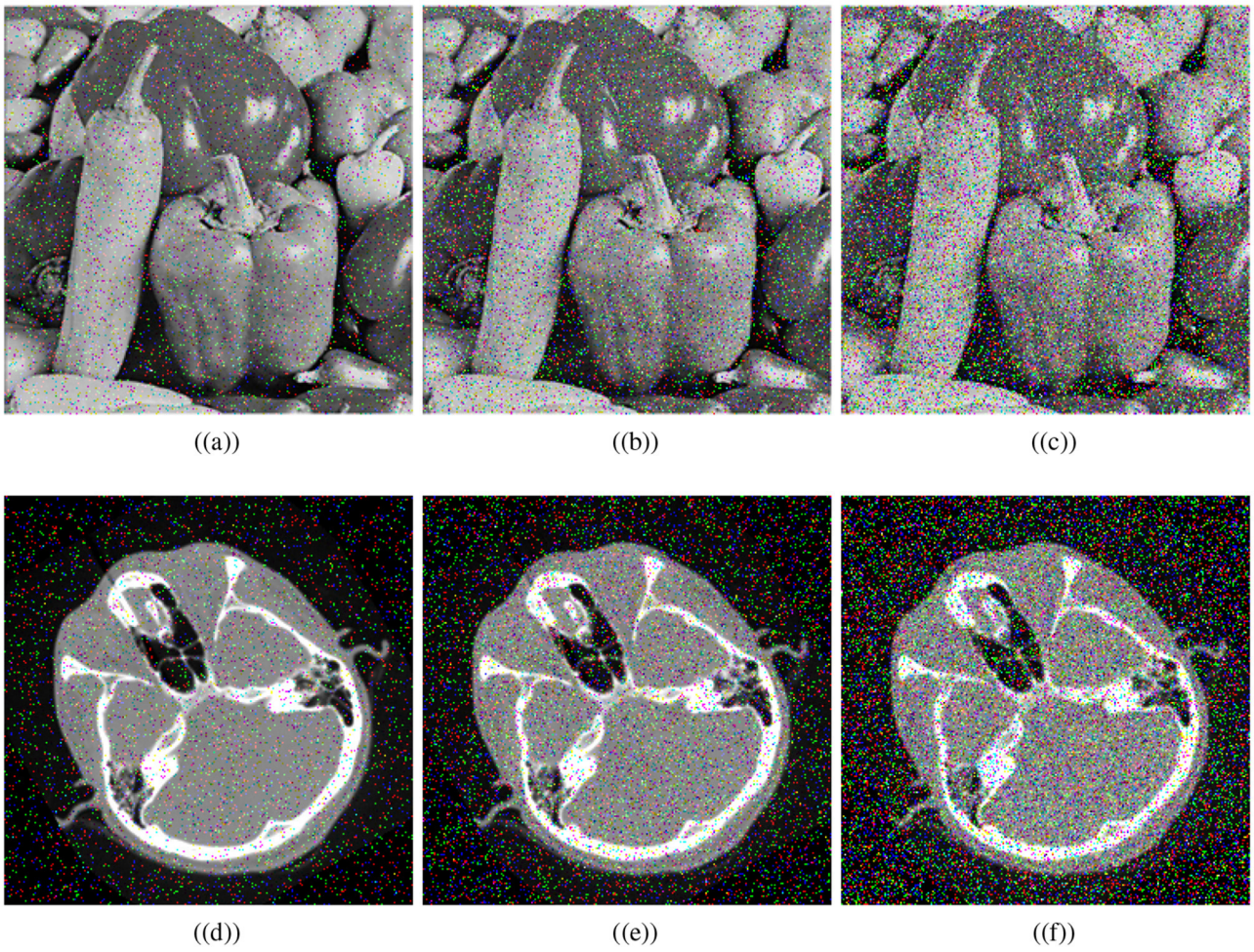

FIGURE 10
Noise results: salt and pepper noise ratios; **(a)** 5%, **(b)** 10%, **(c)** 20%, and **(d–f)** corresponding decrypted images.

mathematically defined as follows (Liu et al., 2024):

$$D(x,y) = \begin{cases} 1, if C_1(x,y) \neq C_2(x,y) \\ 0, if C_1(x,y) = C_2(x,y) \end{cases} \tag{16}$$

$$NPCR = \sum_{x,y} \frac{D(x,y)}{N} \times 100\% \tag{17}$$

$$UACI = \frac{1}{N} \sum_{x,y} \frac{|C_1(x,y) - C_2(x,y)|}{255} 100 \tag{18}$$

where N shows the total number of pixel values and C_1 represents the first encrypted image generated without any change in the original plaintext image while C_2 represents the encrypted image generated after altering just one pixel in the original image. When comparing two images that have been encrypted, the UACI test measures the difference in pixel intensity, whereas the NPCR test measures how frequently the pixels are changed in the plaintext. The calculated NPCR and UACI values for the designed medical image security scheme are illustrated in Table 3. Therefore, the values UACI $>$ 33% and NPCR $>$ 99% confirm that the proposed strategy is resilient to differential attack.

4.7 Noise attack analysis

It has become increasingly important to analyze noise attacks when data is transmitted over open networks due to the presence of noise during transmission. Therefore, the proposed algorithm's effectiveness is determined by comparing the decryption of encrypted images under different noise intensities. Figure 10 shows the recovered images after adding salt and pepper noise of (5%, 10%, and 20%) intensities to the visually secured image. Thus, one can see that the proposed medical encryption scheme can decrypt the noise-polluted ciphertext image, illustrating the robustness of the scheme.

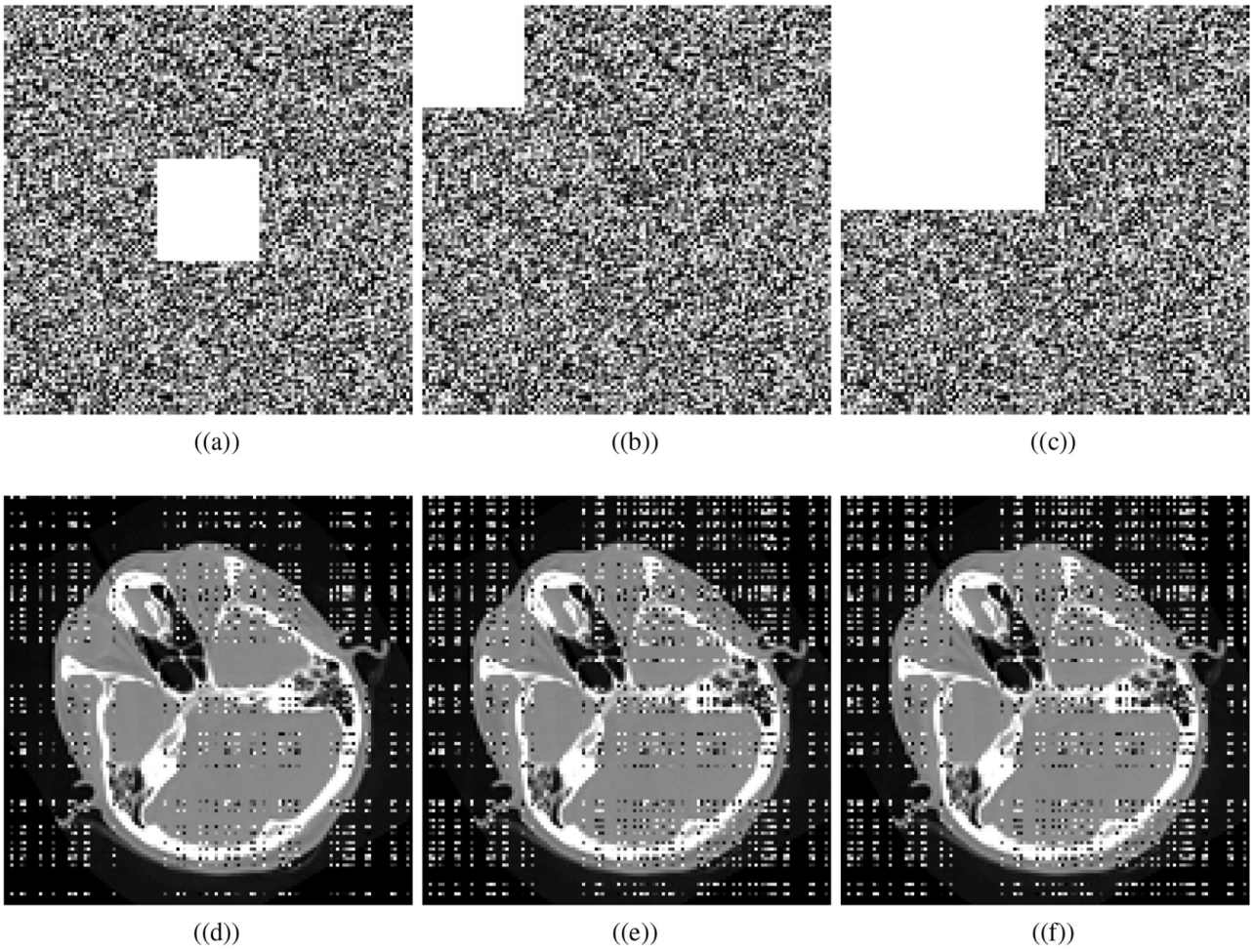

FIGURE 11
Cropping results: Crop ratios of ciphertext cthead image; **(a)** 1/16 (middle), **(b)** 1/16, **(c)** 1/4, and **(d–f)** corresponding decrypted images.

4.8 Occlusion attack analysis

Various factors can cause data to be lost during image transmission over a network. The purpose of occlusion analysis is to determine whether or not an image encryption scheme can recover a plaintext image from a ciphertext image that has been occluded. Different-sized portions of the encrypted image are cropped and decrypted. This analysis can provide insight into how the encryption scheme scrambles plaintext images. Generally, the better the scrambling effect, the more likely the algorithm is to reconstruct the visual characteristics of the plaintext image, even if some part of it has been lost. We cropped the cipher cthead image and visually secured image with the ratios 1/16 (middle), 1/16, and 1/4. Decryption is performed utilizing the presented scheme. Figure 11 shows the cropped ciphertext images and the corresponding decipher images while Figure 12 illustrates the cropped visually secured images and the corresponding decipher images. The visual results clearly deomnstrates that the proposed scheme strongly deciphers the cropped images without causing any noticeable distortion.

4.9 Resilience against classical attacks

Classical attack analysis focuses on identifying and analyzing various types of attacks (known plaintext, chosen plaintext, ciphertext only, and chosen ciphertext) against encrypted images. The key of the chaotic maps is computed based on the plaintext hash value. It is used to determine initial conditions and control parameters. Because of the dependence on plaintext images, the proposed enhanced medical image privacy in IoT with bit-plane level encryption using a chaotic map avoids the classical attacks cited above. Therefore, all random vectors and matrices are determined by plain image bit planes. When a single pixel is changed in the plaintext image, the keystream changes. This will result in a completely different ciphertext image.

4.10 Complexity analysis

Time complexity is a metric used to estimate the running time of an encryption algorithm and generally determine the scheme's

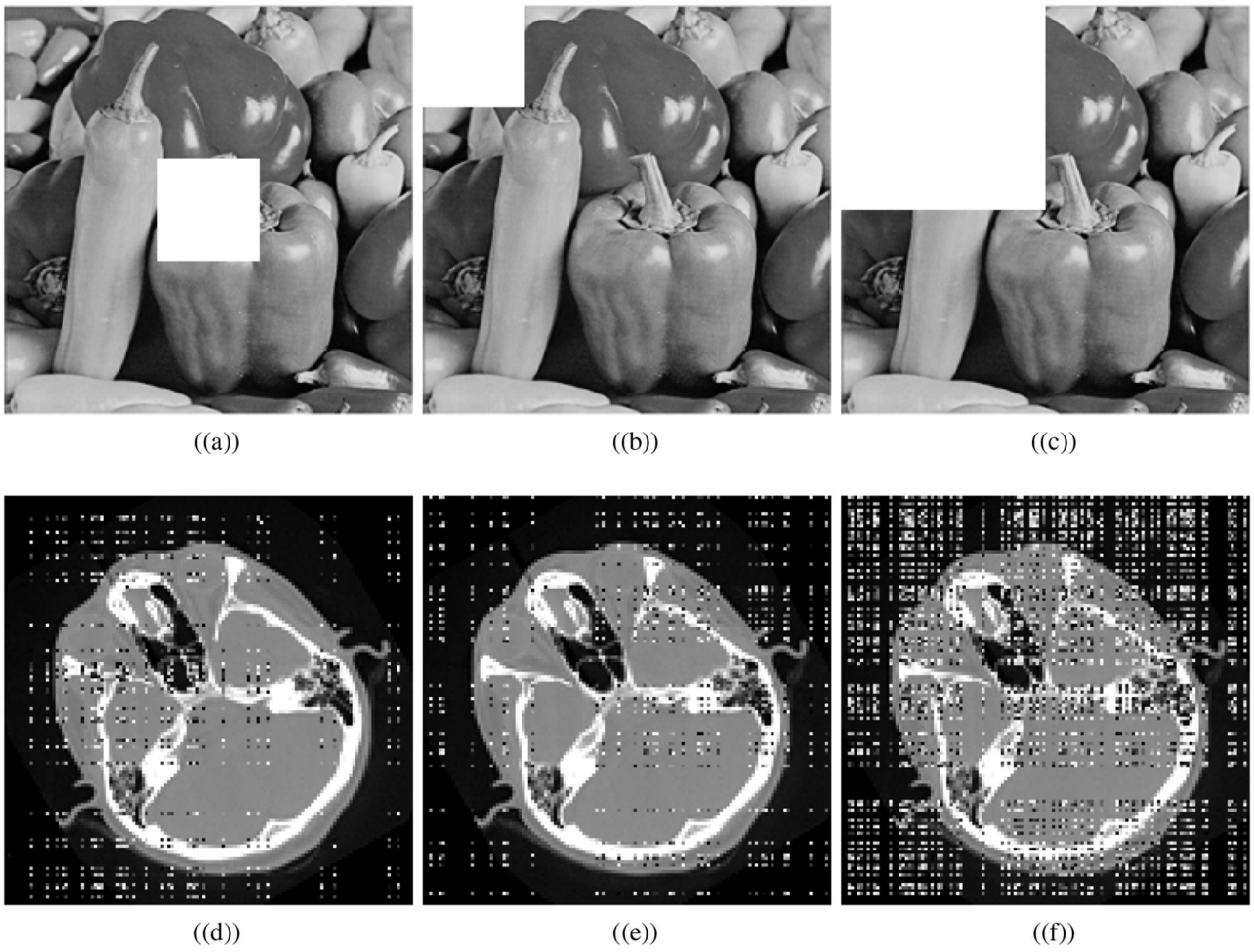

FIGURE 12
Cropping results: Crop ratios of visually meaningful image; **(a)** 1/16 (middle), **(b)** 1/16, **(c)** 1/4, and **(d–f)** corresponding decrypted images.

feasibility. A good algorithm needs to have a short running time. The encryption and decryption results are performed on MATLAB 2018a with Microsoft Windows 10, 4 GB of memory, and a 1 GHz CPU. The cthead and chest images have a size of 128 × 128, while the carrier image has a size of 256 × 256. The proposed scheme takes 0.85s to generate the ciphertext image and 0.62s to produce the visually meaningful ciphertext. Thus, the proposed scheme takes 1.47s to generate the final meaningful ciphertext. The image encryption scheme presented in Kumar and Sharma (2024) takes 0.85s while the scheme discussed in Medani et al. (2025) takes 4.57s to produce the final encrypted images. The designed scheme takes less time than the scheme presented in Medani et al. (2025) and more time than the scheme discussed in Kumar and Sharma (2024).

5 Conclusion

This paper presents a novel and robust medical image encryption scheme for resource-constrained devices. Due to simplicity and exceptional performance in terms of unpredictability, the proposed scheme utilizes 3D Chen chaotic system. The simplicity and excellent performance make the Chen chaotic map an excellent choice for lightweight encryption applications. The designed meaningful bit-plane-level medical image encryption scheme for IoT leverages the pixel scrambling and diffusion characteristics to effectively break pixel relationships, thus, enhancing encryption efficiency and security. To enhance security, the plaintext bit planes are hashed using the Secure Hash Algorithm (SHA-512) to compute the initial conditions of the chaotic map. This dependency on the plaintext images makes the designed scheme resilient against classical attacks (known-plaintext, chosen-plaintext, ciphertext-only, and chosen-ciphertext). As a result, three random vectors for permutation and XOR diffusion are generated. A permutation and XOR operation are applied to each bit-plane to produce a ciphertext plane. After combining the ciphertext bit-planes, the visually secured ciphertext image is now generated by embedding the ciphered image within the carrier image. Extensive evaluations have proven that the designed scheme exhibits a high degree of resilience to attacks, making it particularly suitable for small IoT devices with limited processing power and memory. Computational complexity could be a possible limitation of the designed scheme, as image sizes increase, the encryption process could take longer.

Data availability statement

Interested researchers may contact the author for potential collaboration or for inquiries regarding data access within the constraints of institutional guidelines.

Author contributions

FA: Formal analysis, Methodology, Conceptualization, Writing – original draft, Software, Data curation. WA: Conceptualization, Formal analysis, Methodology, Writing – original draft. TZ: Formal analysis, Methodology, Validation, Writing – review & editing. IN: Formal analysis, Methodology, Visualization, Writing – original draft. AA: Investigation, Supervision, Validation, Visualization, Writing – review & editing, Project administration. NG: Formal analysis, Investigation, Project administration, Supervision, Writing – review & editing. AQ: Formal analysis, Writing – review & editing, Methodology, Resources, Software.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP.2/245/46).

Acknowledgments

The authors extend their appreciation to the Deanship of Research and Graduate Studies at King Khalid University for funding this work through Large Group Project under grant number (RGP.2/245/46).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

Al-Haj, A., Abandah, G., and Hussein, N. (2015). Crypto-based algorithms for secured medical image transmission. *IET Inf. Secur.* 9, 365–373. doi: 10.1049/iet-ifs.2014.0245

Alvarez, G., and Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* 16, 2129–2151. doi: 10.1142/S0218127406015970

Aman, A. H. M., Yadegaridehkordi, E., Attarbashi, Z. S., Hassan, R., and Park, Y.-J. (2020). A survey on trend and classification of internet of things reviews. *IEEE Access* 8, 111763–111782. doi: 10.1109/ACCESS.2020.3002932

Belazi, A., Talha, M., Kharbech, S., and Xiang, W. (2019). Novel medical image encryption scheme based on chaos and dna encoding. *IEEE Access* 7, 36667–36681. doi: 10.1109/ACCESS.2019.2906292

Bhonge, H. N., Ambat, M. K., and Chandavarkar, B. (2020). "An experimental evaluation of sha-512 for different modes of operation," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (IEEE), 1–6. doi: 10.1109/ICCCNT49239.2020.9225559

Cao, W., Zhou, Y., Chen, C. P., and Xia, L. (2017). Medical image encryption using edge maps. *Signal Proc.* 132, 96–109. doi: 10.1016/j.sigpro.2016.10.003

Chu, L., Su, Y., Zan, X., Lin, W., Yao, X., Xu, P., et al. (2024). A deniable encryption method for modulation-based DNA storage. *Comput. Life Sci.* 16, 872–881. doi: 10.1007/s12539-024-00648-5

Dridi, M., Hajjaji, M. A., Bouallegue, B., and Mtibaa, A. (2016). Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Process.* 10, 830–839. doi: 10.1049/iet-ipr.2015.0868

Gan, Z., Xiong, B., Pang, Z., Chai, X., Jiang, D., and He, X. (2024). A visually secure image encryption scheme using newly designed 1d sinusoidal chaotic map and p-tensor product compressive sensing. *Nonlinear Dyn.* 112, 2979–3001. doi: 10.1007/s11071-023-09203-1

Hanchate, R., and Anandan, R. (2024). Medical image encryption using hybrid adaptive elliptic curve cryptography and logistic map-based DNA sequence in IoT environment. *IETE J. Res.* 70, 5734–5749. doi: 10.1080/03772063.2023.2268578

Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.-H. A., Habib, S., et al. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. *IEEE Access* 9, 47731–47742. doi: 10.1109/ACCESS.2021.3061710

Hu, J., Jiang, H., Chen, S., Zhang, Q., Xiao, Z., Liu, D., et al. (2024). Wishield: privacy against wi-fi human tracking. *IEEE J. Select. Areas Commun.* 42, 2970–2984. doi: 10.1109/JSAC.2024.3414597

Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., and Abu-Elyazeed, M. F. (2018). Generalized double-humped logistic map-based medical image encryption. *J. Adv. Res.* 10, 85–98. doi: 10.1016/j.jare.2018.01.009

Jain, K., Titus, B., Krishnan, P., Sudevan, S., Prabu, P., and Alluhaidan, A. S. (2024). A lightweight multi-chaos-based image encryption scheme for IoT networks. *IEEE Access* 12, 62118–62148. doi: 10.1109/ACCESS.2024.3377665

Kanwal, S., Inam, S., Nawaz, Z., Hajjej, F., Alfraihi, H., and Ibrahim, M. (2024). Securing blockchain-enabled smart health care image encryption framework using tinkerbell map. *Alexandria Eng. J.* 107, 711–729. doi: 10.1016/j.aej.2024.08.115

Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., and Quaynor, N. N. (2015). A cryptographic technique for security of medical images in health information systems. *Procedia Comput. Sci.* 58, 538–543. doi: 10.1016/j.procs.2015.08.070

Khan, J. S., and Ahmad, J. (2019). Chaos based efficient selective image encryption. *Multidimens. Syst. Signal Process.* 30, 943–961. doi: 10.1007/s11045-018-0589-x

Khan, J. S., Ahmad, J., Abbasi, S. F., and Kayhan, S. K. (2018). "DNA sequence based medical image encryption scheme," in *2018 10th Computer Science and Electronic Engineering (CEEC)* (IEEE), 24–29. doi: 10.1109/CEEC.2018.8674221

Khan, J. S., Ahmed, S. S., Haq, F. U., Tariq, N., Ahmad, J., and Ashraf, M. (2024). "A robust visually secure bit plane image encryption using chaotic map and sha-512," in *2024 3rd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (IEEE), 1–6. doi: 10.1109/ETECTE63967.2024.10823709

Khan, J. S., Boulila, W., Ahmad, J., Rubaiee, S., Rehman, A. U., Alroobaea, R., et al. (2020). Dna and plaintext dependent chaotic visual selective image encryption. *IEEE Access* 8, 159732–159744. doi: 10.1109/ACCESS.2020.3020917

Kumar, S., and Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artif. Intell. Rev*. 57:87. doi: 10.1007/s10462-024-10719-0

Lai, Q., and Hua, H. (2025). Secure medical image encryption scheme for healthcare IoT using novel hyperchaotic map and DNA cubes. *Expert Syst. Appl*. 264:125854. doi: 10.1016/j.eswa.2024.125854

Liu, W., Wang, H., Chen, Y., and Sun, K. (2024). A new image encryption scheme based on block compressive sensing and chaotic laser system for IoT. *Eur. Phys. J. Plus* 139:473. doi: 10.1140/epjp/s13360-024-05221-z

Medani, M., Said, Y., Othman, N. A., Yuldashev, F., Kchaou, M., Aldawood, F. K., et al. (2025). Chaos-based novel watermarked satellite image encryption scheme. *Comput. Model. Eng. Sci*. 143, 1049–1070. doi: 10.32604/cmes.2025.063405

Nadhan, A. S., and Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in iot healthcare applications. *Biomed. Signal Process. Control* 88:105511. doi: 10.1016/j.bspc.2023.105511

Porras, J., Pänkäläinen, J., Knutas, A., and Khakurel, J. (2018). "Security in the internet of things-a systematic mapping study," in *Proceedings of the 51st Hawaii International Conference on System Sciences*. doi: 10.24251/HICSS.2018.473

Qi, G., Chen, G., Du, S., Chen, Z., and Yuan, Z. (2005). Analysis of a new chaotic system. *Physica A* 352, 295–308. doi: 10.1016/j.physa.2004.12.040

Sathananthavathi, V., Ganesh Kumar, K., and Sathish Kumar, M. (2024). Secure visual communication with advanced cryptographic and image processing techniques. *Multimed. Tools Appl*. 83, 45367–45389. doi: 10.1007/s11042-023-17224-6

Singh, D., and Kumar, S. (2025). Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps. *Expert Syst. Applic*. 274:126883. doi: 10.1016/j.eswa.2025.126883

Trujillo-Toledo, D. A., López-Bonilla, O. R., García-Guerrero, E. E., Esqueda-Elizondo, J. J., Cárdenas-Valdez, J. R., Tamayo-Pérez, U. J., et al. (2023). Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps. *Integration* 90, 131–145. doi: 10.1016/j.vlsi.2023.01.008

Wang, K., Wu, X., Wang, H., Kan, H., and Kurths, J. (2021). New color image cryptosystem via sha-512 and hybrid domain. *Multimed. Tools Appl*. 80, 18875–18899. doi: 10.1007/s11042-021-10511-0

Ye, G., and Huang, X. (2015). An image encryption algorithm based on autoblocking and electrocardiography. *IEEE MultiMedia* 23, 64–71. doi: 10.1109/MMUL.2015.72

Zhang, D., Yan, C., Duan, Y., Liang, S., Wu, J., and Li, T. (2024). A fast visually meaningful image encryption algorithm based on compressive sensing and joint diffusion and scrambling. *Multim. Tools Applic*. 83, 70693–70725. doi: 10.1007/s11042-024-18343-4