




A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map

Bin Zhang^{1,2} · Bahbibbi Rahmatullah¹  · Shir Li Wang¹ · Zhaoyan Liu³

Received: 13 February 2022 / Revised: 18 April 2022 / Accepted: 29 August 2022 /

Published online: 23 September 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Modern medical examinations have produced a large number of medical images. It is a great challenge to transmit and store them quickly and securely. Existing solutions mainly use medical image encryption algorithms, but these encryption algorithms, which were developed for ordinary images, are time-consuming and must cope with insufficient security considerations when encrypting medical images. Compared with ordinary images, medical images can be divided into the region of interest and the region of background. In this paper, based on this characteristic, a plain-image correlative semi-selective medical image encryption algorithm using the enhanced two dimensional Logistic map was proposed. First, the region of interest of a plain medical image is permuted at the pixel level, then for the whole medical image, substitution is performed pixel by pixel. An ideal compromise between encryption speed and security can be achieved by full-encrypting the region of interest and semi-encrypting the region of background. Several main types of medical images and some normal images were selected as the samples for simulation, and main image cryptanalysis methods were used to analyze the results. The results showed that the cipher-images have a good visual quality, high information entropy, low correlation between adjacent pixels, as well as uniformly distribute histogram. The algorithm is sensitive to the initial key and plain-image, and has a large key space and low time complexity. The time complexity is lower when compared with the current medical image full encryption algorithm, and the security performance is better when compared with the current medical image selective encryption algorithm.

✉ Bahbibbi Rahmatullah
bahbibbi@fskik.upsi.edu.my

¹ Data Intelligence and Knowledge Management, Faculty of Arts, Computing and Creative Industry, Sultan Idris Education University (UPSI), Tanjong Malim, Perak, Malaysia

² School of Computer Science, Baoji University of Arts and Sciences, Baoji, China

³ School of Cyber Engineering, Xidian University, Xi'an, China

Keywords Medical image · Image encryption · Selective encryption · Partial encryption · Chaotic map · SHA-256

1 Introduction

1.1 Background

Modern medical examinations have produced a large number of medical images such as X-ray, computed tomography (CT), magnetic resonance imaging (MRI), ultrasound and positron emission tomography (PET) [9, 11, 35, 38, 55, 56, 69, 71]. These medical images are stored in digital format and may need to be transmitted between doctors and hospitals over an open public network [16]. Transmitting medical images over open networks is risky and easily accessed illegally by hackers [5, 8, 23]. Safe and effective medical services can only be achieved when these medical data are highly secure [38]. In this case, many countries have passed legislation to regulate the security of medical images [19, 70].

In early research, the protection of medical image privacy was mostly based on classical encryption algorithms, which include classical public-key cryptography algorithms, such as RSA cryptography [31] and ElGamal cryptography [66], and classical symmetric encryption algorithms, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) [49] and International Data Encryption Algorithm (IDEA) [57]. To reduce the encryption time of classical algorithms, the research focus on the frontier of image encryption technology which are currently the chaotic map-based encryption algorithms [75]. Among the algorithms, the most important structure is the “Confusion-Diffusion”, which was proposed by Fridrich [25]. Confusion includes two basic operations, “Permutation” and “Substitution.” Permutation, also called “Shuffle” or “Scrambling” in different literature, aims to permute the position of pixels in a medical image and reduce the correlation of adjacent pixels. Meanwhile, substitution adjust the values of pixels to alter the statistical characteristics of images. Diffusion can associate each part of the image with each part of the key, which can improve plain-image sensitivity and key sensitivity, and enhance the ability to resist differential attack. By using this structure, many medical image full-encryption algorithms have emerged [14, 18, 26, 29, 41, 42, 44, 58, 60, 61, 71].

In recent years, to further increase the encryption speed of medical image encryption algorithms, many selective or partial encryption schemes have been proposed for the uneven distribution of medical image information. Abdmouleh, M. K. et al. proposed an algorithm on transform domain, in which medical images were first decomposed by using the discrete wavelet transform (DWT) with different levels, and then the LL sub-band with maximum information content was encrypted [3]. Zhou, J. et al. proposed another algorithm to partially encrypting the transform domain, while the two-dimensional lifting wavelet transform (2D LWT) was adopted [78]. Two selective encryption algorithms were proposed by Ravichandran, D. et al. and Prabhavathi, K. respectively, in which the rectangle region in the central part of a medical image is manually selected as the region of interest (ROI) for encryption [52, 59]. In another work, a 4D Cat map-based selective encryption scheme was designed by Kansa, A., & Ghebleh, M., the algorithm needs to run multiple rounds, and each round of encryption consists of permutation and substitution [34]. Khashan, O. A., & Alshaikh, M. proposed a lightweight chaotic map-based encryption algorithm to encrypt the edge image of medical images [36]. In literature [51], based on cellular automata (CA), Ping P. et al. proposed a method to encrypt the ROI of medical images. Unfortunately, none of the

above methods have any processing on the non-selected region of medical images, resulting in poor security of cipher-images. Their typical features are that the shape of the selected region can be easily seen from the cipher image, and all information about the unselected region can be obtained directly from the cipher-image.

Noura, M. et al. proposed a middle-full encryption mode, in which the ROI of medical images was first encrypted by adopting substitution operation, and then the whole medical image was encrypted by using permutation operation [50]. Manikandan, V. et al. proposed a semi-full encryption scheme based on the transform domain [46]. Firstly, the whole medical image is permuted using the Bülban map, and then substitute the LL sub-band, which is extracted by using 5/3 lifting transform, with high information. However, these two schemes did not change the statistical characteristics of the region of not interest (RONI), leading to risks of statistical attacks.

Another study aimed at the characteristics of different information amounts in different bit-planes of medical images, a multi-chaotic maps-based medical image semi-full encryption algorithm was designed [21]. In this algorithm, according to the information amount of each bit-plane, different rounds of permutation were run in the bit-plane itself respectively, and then the whole medical image was encrypted by using substitution operation. However, the algorithm needs to run too many rounds, even up to 100, which costs a lot of time when encrypting medical images. Another bit-plane based scheme was proposed by Muthu J. S. et al. [48]. Four bit-planes with the high information content of medical images were selected to be permuted, and then the whole medical image was substituted. Compared with the scheme [21], the processing speed is significantly improved.

DNA computing and the Dual Hyperchaotic map had also been proposed for selective encryption algorithm [4]. First, the selected region of a medical image was encrypted by using permutation operation and then encrypted the whole image with substitution operation. However, the actual DNA computing requires additional bio-computing equipment. Besides, there will be additional computing overhead when simulations are run on computers. Shafique A. et al. proposed a 3-level structure to encrypt medical images [63]. In the first and third levels, four bit-planes with high information content were selected to be permuted inner the bit-planes respectively. In the second level, the LL sub-band of the transform domain was selected to be substituted. However, the efficiency of the scheme is low, and it will take more than 3 seconds to encrypt a medical image. Manikandan, V et al. also proposed a 3-level medical image encryption structure [45]. In the first and third levels, the whole medical image was encrypted by using the “permutation-substitution” structure. And in the second level, the classical RC6 algorithm was used to encrypt the LL sub-band of the transform domain. However, the time complexity of the method is so high that it takes tens of seconds to encrypt a medical image.

Literature review shows that the existing medical image selective encryption methods have problems of inadequate security and high computing complexity. Therefore, it is an urgent need to develop a fast and secure selective encryption algorithm for medical images.

1.2 Contributions

In this work, a plain-image correlative semi-selective medical image encryption algorithm using an enhanced 2D-Logistic map was proposed. The main contributions are as follows:

- *Based on the original 1D-Logistic chaotic map, an enhanced 2D-Logistic chaotic map was proposed, which not only increased the number of chaotic control parameters and chaotic initial values but also expanded the value range of chaotic parameters and chaotic sequences.*

- *A plain-image correlative semi-selective medical image encryption algorithm using the enhanced 2D-Logistic map was designed.*
- *The security and time complexity of the proposed algorithm were analyzed objectively.*

The work is demonstrated as follows. Section 2 defines the detail of the enhanced 2-D logistic chaotic map, analyzes its chaos, and then briefly introduces the Secure Hash Algorithm SHA-256. Section 3 defines the detail of the proposed plain-image correlative semi-selective medical image encryption algorithm. Section 4 illustrates the simulation results of the algorithm and discusses its security and time complexity. Section 5 defines the conclusion of the work.

2 Preliminaries

2.1 The original 1-D logistic chaotic map

The Logistic map, also known as the insect population model in ecology [21], is a typical nonlinear chaotic system, which is highly sensitive to the initial state [1] and can produce complex chaotic behaviors [33]. This system has been widely used in the research field of medical image encryption [1, 7, 8, 10, 12, 17, 20–22, 24, 27, 28, 33, 37, 39, 40, 43, 47, 53, 54, 62, 65, 68, 73, 74, 76, 77]. The original 1-D Logistic chaotic map can be defined by the following Eq. 1.

$$x_{n+1} = ax_n(1-x_n) \quad (1)$$

Here:

$$n \in N^+$$

- x_n is the first n iteration result of the system, and $x_n \in (0, 1)$.
- a is the chaotic control parameter, and $a \in (0, 4]$.

The chaotic bifurcation diagram of the original 1-D Logistic chaotic map is illustrated in Fig. 1. It can be seen that the Logistic map is in chaos when the chaotic control parameter value is $a \in (3.6, 4]$ [32], that is to say, when the chaotic iteration continues, the generated chaotic sequence will be an aperiodic and non-convergent pseudo-random sequence [21]. On the contrary, when the chaotic control parameter value is $a \in (0, 3.6]$, the Logistic map shows determinism, that is to say, when the number of chaotic iterations is large enough, the result sequence will converge to a certain constant value [21]. Furthermore, it can be seen that even when the chaotic control parameter value is $a \in (3.6, 4]$, there are still some periodic (non-chaotic) windows. In order to solve this problem, the traditional works usually select the chaotic control parameter to ensure the chaotic characteristics of cryptosystems [76].

2.2 The enhanced 2-D logistic chaotic map

The chaotic sequence value distribution of the original 1-D Logistic chaotic map is not uniform, and there is a problem of small keyspace when it is applied to cryptosystems. In some research work, multi chaotic systems combined with the Logistic chaotic map have been proposed for medical image encryption, such as Logistic-Tent map [58], Logistic-Sine map [2, 16, 29, 58], Double Humped Logistic map [30], and Logistic-Chebyshev map [13]. In some other research works, the

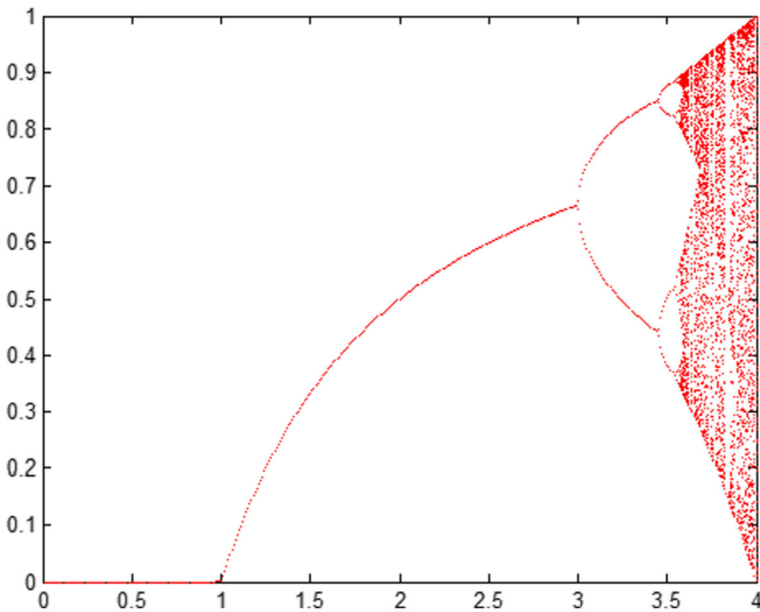


Fig. 1 The bifurcation diagram of the original 1-D Logistic chaotic map

original 1-D Logistic chaotic map was extended to multi-dimensional, such as 2-D Logistic chaotic map [64], 3-D Logistic chaotic map [15], 4-D Logistic chaotic map [67]. However, the problems of chaotic windows and non-uniform chaotic sequence value distribution have not been solved well. Besides, it has not established organic connections among multi chaotic systems.

In this work, an enhanced 2-D Logistic chaotic map was proposed, which can be defined by the following Eq. 2.

$$\begin{cases} x_{k+1} = f(a, x_k, y_k) - [f(a, x_k, y_k)] \\ y_{k+1} = f(b, y_k, x_k) - [f(b, y_k, x_k)] \end{cases} \quad (2)$$

Here:

- The symbol [...] means to take the integer part, and the fractional part is discarded directly.
- $k \in \mathbb{N}^+$; $x, y \in (0, 1)$; $a, b \in \mathbb{R}^+$.

$$f(a, x_k, y_k) = ax_k(1-x_k) + 1024(y_k).$$

$$f(b, y_k, x_k) = by_k(1-y_k) + 1024(x_k).$$

In the case of chaotic control parameters value range is $0 < a, b \leq 10$, the bifurcation diagram of components x and y are illustrated in Fig. 2.

It can be seen that the enhanced 2-D Logistic chaotic map increases the number of initial values and chaotic control parameters, the system shows chaos when the control parameters

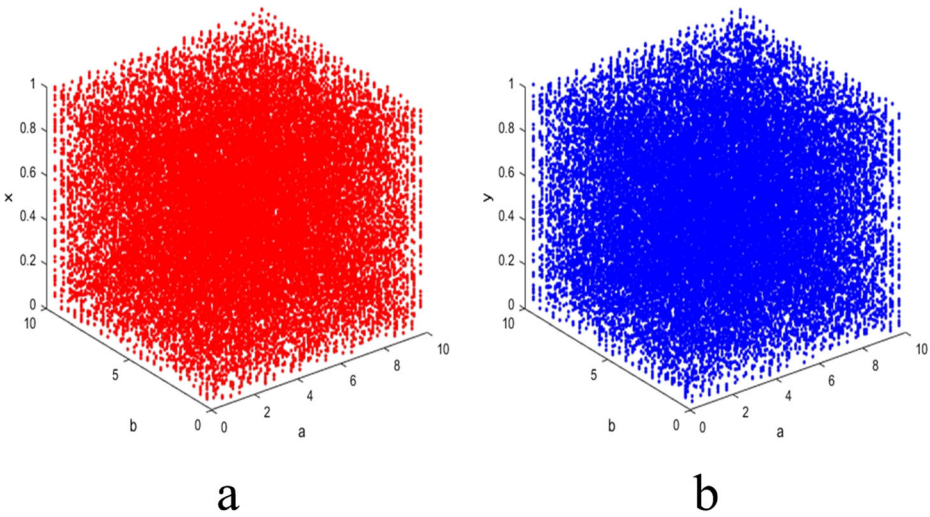


Fig. 2 The bifurcation diagram of the enhanced 2-D Logistic chaotic map (a: bifurcation diagram of component x, b: bifurcation diagram of component y)

are in a wider range of values, the values of chaotic sequences are distributed uniformly in the interval [0,1], and chaotic windows are eliminated.

2.3 Secure hash algorithm

The Secure hash algorithm 256 (SHA-256) can map a message M of any length to a 256-bits hash code SHA-256(M). When the input M changes slightly to M', the hash code SHA-256(M') changes completely in an unpredictable way. Besides, the SHA-256 algorithm is unidirectional, which means it is easy to compute SHA-256(M) from the input M, while it is computationally infeasible to compute M from SHA-256(M). In addition, the SHA-256 has error detection capability, which can be used to verify the integrity of a message. In this work, the plain medical image is used as the input of SHA-256, and the output of 256-bits length is divided into 32 pieces, where each piece is 8-bits length, as shown in Eq. 3.

$$SHA-256(image) = s1, s2, s3, \dots, s32 \tag{3}$$

Here:

- *image* is the binary code of the input image.
- *s(n)* is the NTH segment of the hash sequence.

3 The proposed plain-image correlative semi-selective medical image encryption algorithm

In this work, a plain-image correlative semi-selective medical image encryption algorithm using the proposed chaotic map is designed. The flow chart of the algorithm is shown in

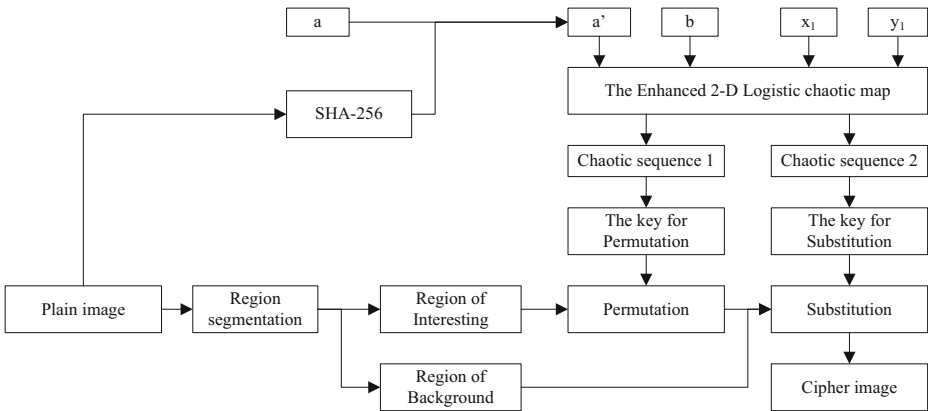


Fig. 3 Structure of the proposed plain-image correlative semi-selective medical image encryption algorithm

Fig. 3. First, the plain medical image is read, and the SHA-256 value of the image is calculated. Then chaotic initial values and control parameters of the enhanced 2D-Logistic chaotic map are generated randomly. Two sets of plain-image correlative chaotic sequences are obtained by using enough round iterations of the enhanced 2D-Logistic chaotic map. The following step is based on the first set of chaotic sequence, where the permutation key is generated and used for encrypting the ROI of the medical image. The semi-encrypted image can be obtained by merging the region of background (ROB) and the permuted ROI. Finally, based on the second set of chaotic sequences, the substitution key is generated, which is used to encrypt the semi-encrypted image to obtain the final cipher medical image.

The detailed implementation of the algorithm includes the following steps:

Step1: Select a plain medical image: $Img (M, N)$.

- Here M is the number of rows of the Img and N is the number of columns of the Img

Step2: Segment the medical image Img into $Img(ROI)$ and $Img(ROB)$, and count the pixel number of $Img(ROI)$.

$$Img(ROI), Img(ROB) = Segment(Img).$$

$Count =$ the pixel number of $Img(ROI)$

Step3: Calculate the SHA-256 value of image Img .

$$SHA-256(Img) = s1, s2, s3, \dots, s32$$

Step4: Generate chaotic control parameters and chaotic initial values randomly, with the precision of 15 decimal places, where the parameter a' requires plain-image correlation.

$$a, b, x_1, y_1 = random$$

$$\begin{aligned}
 a' &= a + (s1 + \dots + s5)/(5 \times 256) \\
 &\quad + (s6 + \dots + s10)/(5 \times 256^2) \\
 &\quad + (s11 + \dots + s15)/(5 \times 256^3) \\
 &\quad + (s16 + \dots + s20)/(5 \times 256^4) \\
 &\quad + (s21 + \dots + s25)/(5 \times 256^5) \\
 &\quad + (s26 + \dots + s30)/(5 \times 256^6)
 \end{aligned}$$

Step5: Generate two sets of plain-image correlated chaotic sequences CS1 and CS1 according to Eq. 2, and the number of iterations rounds is $M \times N + 10000$.

$$CS1, CS2 = Chaoticmap(a', b, x_1, y_1)$$

Step6: Generate the encryption key. The chaotic sequences CS1 are selected according to the size of ROI, which is sorted to generate the key for the permutation. The chaotic sequences CS2 are amplified 2^d times and then take the integer part to generate the key for the substitution.

$$Pkey = sort(CS1(10001), CS1(10002), \dots, CS1(10,000 + Count))$$

$$Skey = [(CS2(10001), CS2(10001), \dots, CS2(10000 + M \times N)) \times 2^d]$$

-Here, d is the color depth of the Img , and $[]$ is the symbol of taking the integer part.

Step7: Encrypt the ROI by permutating the pixel position.

$$P(ROI) = Permutation(Img(ROI), Pkey)$$

Step8: Merge permuted ROI with ROB.

$$P(Img) = Merge(P(ROI), Img(ROB))$$

Step9: Encrypt the $P(Img)$ by substituting its pixel one by one to achieve the final encryption image.

$$Cipher(Img) = (P(Img) + Skey) \bmod 2^d.$$

The decryption algorithm is the inverse of the encryption algorithm, and the structure is illustrated in Fig. 4. First, the cipher medical image is read and the decryption keys are regenerated according to a, b, x_1, y_1 and $SHA-256(Img)$, which can be obtained from the secret key transfer channel. Then, according to the opposite steps of the encryption algorithm, using inverse substitution operation to the entire cipher-image and inverse permutation operation to the ROI respectively, to get the decrypted medical image. Finally, the SHA-256 value of the decrypted image was calculated and compared with the original $SHA-256(Img)$ to verify the integrity of the medical image.

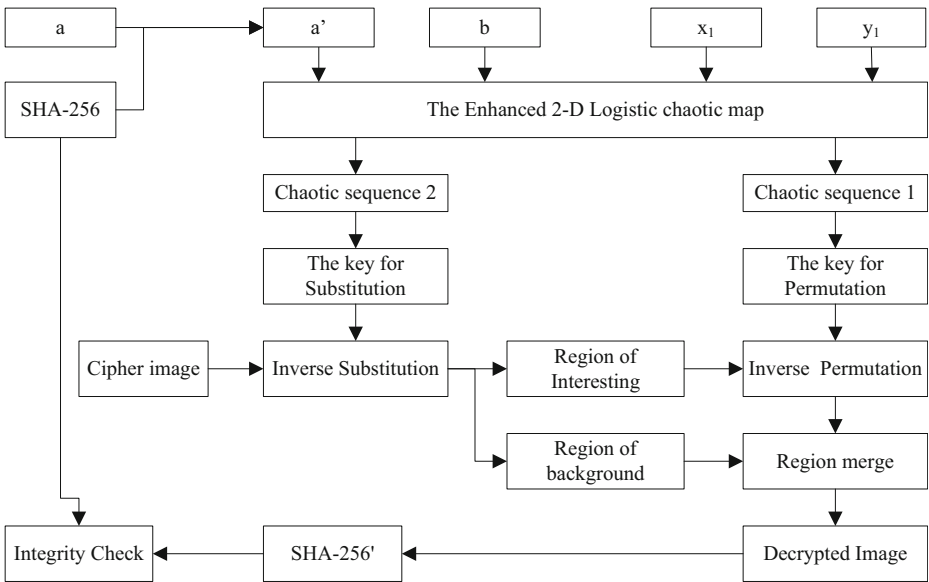


Fig. 4 Structure of the decryption algorithm

4 Simulation results and analysis

4.1 Simulation platform and data samples

This research is algorithm research about medical image encryption. Therefore, the simulation platforms required are only computer hardware and software. The details of them are listed in Table 1.

This research is algorithm research about medical image encryption. Therefore, the main types of medical images, including, X-ray, CT, MRI, ultrasound, PET and COVID-19 virus images, are selected as simulation samples. In addition, some normal images are also used as samples to further analyze the proposed algorithm. The basic attributes of these simulation samples are shown in Table 2, and the plain images of them are illustrated in Fig. 5.

4.2 Simulation results and analysis

In this section, the encryption results of the simulation samples are illustrated and analyzed. The analysis methods used in the research include two main categories: confidentiality analysis and time complexity analysis.

Table 1 The Software and hardware platform used in simulations

Platform	Details
Software	The operating system: Window7 64bit The simulation software: MATLAB r2016a
Hardware	Platform: HP personal computer CPU: Inter(R) Core(TM) i7-5500u 2.4GHZ Memory: 8GB

Table 2 Description of simulation images samples

Image ID	Image type	Body part	Image size
a	X-ray	Foot	512 × 512
b	CT	Brain	256 × 256
c	MRI	Head	256 × 256
d	Ultrasound	Fetus	512 × 512
e	PET	Brain	256 × 256
f	Virus	COVID-19	512 × 512
g	Normal image	Lena	512 × 512
h	Normal image	Peppers	256 × 256

4.2.1 Confidentiality analysis

In confidentiality analysis, four different types of analysis methods are mainly adopted. (1) The visual quality analysis of cipher-images. (2) Statistical analysis, including histogram analysis, information entropy analysis, and correlation analysis of adjacent pixels. (3) The key analysis, including key space and key sensitivity analysis. (4) Chosen plain-image analysis.

Cipher-image visual quality analysis Using the proposed algorithm to process samples in Fig. 5, the permutation results of ROI, final encryption results, and corresponding decryption results are illustrated in Fig. 6. Since Fig. 5g and h are normal images without ROB, the whole images of them were treated as ROI in the permutation step. Here the chaotic control parameters and chaotic initial value are randomly selected as Table 3. It can be seen that the ROI after permutation processing has obtained primary protection. After substitution processing for the whole image, any subjective visual information cannot be seen from the cipher-image. This means that the quality of the cipher-image subjective visual is good. Meanwhile, there is no visual difference between the decrypted image and the original plain image.

Statistical analysis Histogram analysis The pixel distribution histogram can intuitively describe the number of pixels with different values in an image. For an ideal cipher-image, it should have a

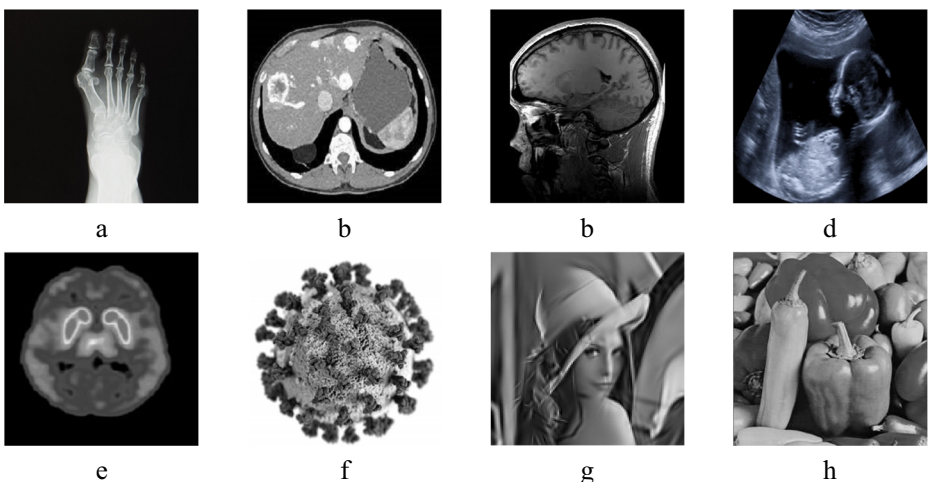


Fig. 5 Simulation medical image and normal image samples (a: Foot X-ray; b: Brain CT; c: Head MRI; d: Fetus Ultrasound; e: Brain PET; f: COVID-19 virus; g: lena; h: peppers)

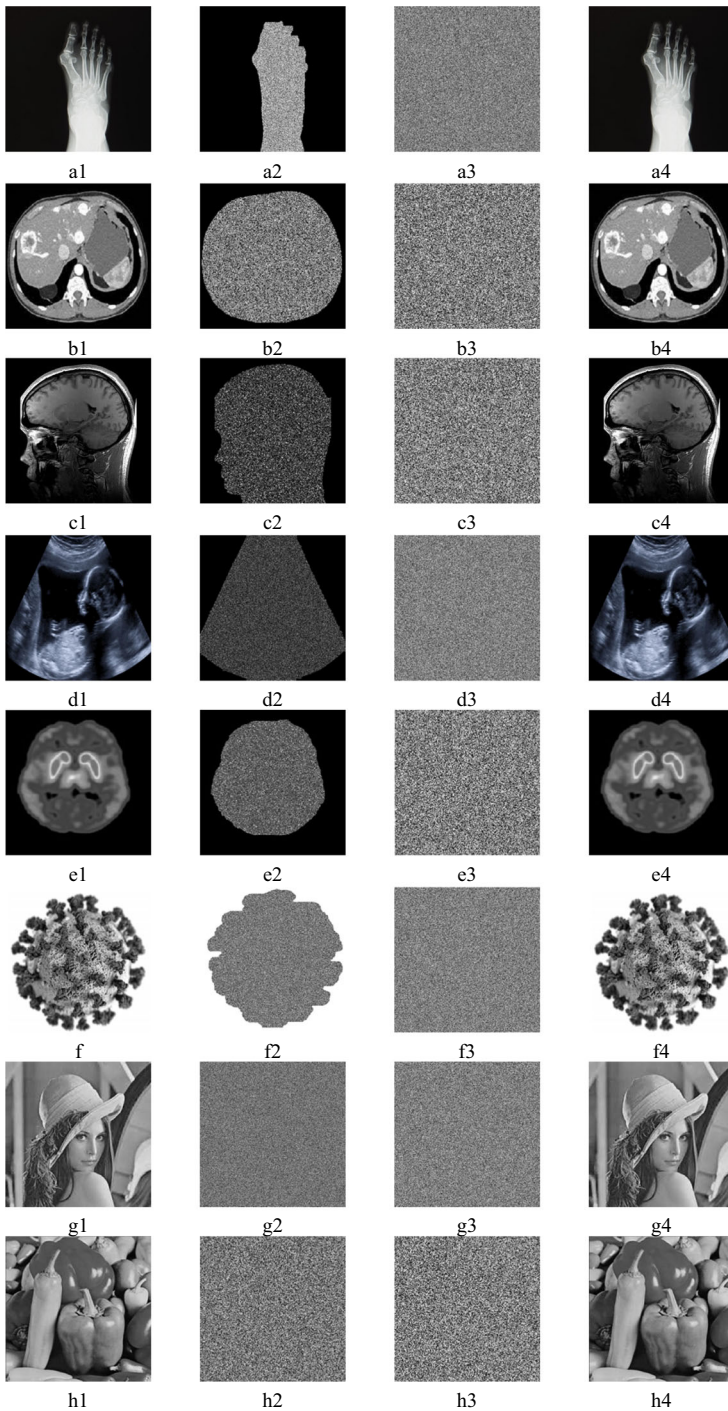


Fig. 6 The visual quality of sample images (1st column: plain-image; 2nd column: permutation result; 3rd column: final encryption result; 4th column: decrypted image)

Table 3 The chaotic control parameters and chaotic initial value

	<i>a</i>	<i>b</i>	<i>x</i> ₁	<i>y</i> ₁
Value	3.889632578965258	2.895365874521023	0.723657891234568	0.589632147852589

completely different histogram from the corresponding plain-image, and generally speaking, its histogram should be approximately uniform distributed. The histograms of sample images are analyzed, and the results are illustrated in Fig. 7. It can be seen that each cipher-image has a uniform distributed histogram, which means that the algorithm does well with histogram analysis.

Information entropy analysis Entropy is a quantitative measure of disorder or uncertainty in a system. The higher of the information entropy value, the more chaotic of the system. For an image *I*, its information entropy value can be calculated as Eq. 4:

$$Entropy(I) = - \sum_0^{2^d-1} P(I_k) \log_2 P(I_k) \tag{4}$$

Here:

- *P(Ik)* is the proportion of the pixel with the value of *k* in the total number of pixels,
- *d* is the color depth of image *I*.
- Σ is the continuous addition symbol.

According to Eq. 4, it is easy to know that an image with a color depth of *d* can have the maximum information entropy value of *d*. The larger the result value, the better the randomness of the cipher-image, and the higher security of the algorithm. The information entropy value of sample images is calculated, and the results are listed in Table 4. It can be seen that the information entropy of cipher-image is very close to the ideal value 8, which indicates that the number of pixels with different pixel values is very close to uniform distribution from a quantitative perspective. Cryptanalysts can hardly get any useful information by using information entropy analysis.

Correlation analysis of adjacent pixels Correlation analysis of adjacent pixels is another important statistical analysis method. For visually meaningful images, the correlation between adjacent pixels is usually high because their pixel values are usually close. A good medical image encryption algorithm should ensure that the correlation between adjacent pixels of the cipher-image is low enough. The correlation of adjacent pixels can be calculated from horizontal, vertical, and diagonal directions as Eq. 5.

$$cor_{x,y} = \frac{E(x-E(x))(y-E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

Here:

- *E()* means the Expectation.
- *D()* means the square deviation.

It can be known from the mathematical properties of Eq. 5 that the value of *cor*_{*x, y*} must be between [−1, 1]. The value is closer to 0, the correlation between the adjacent pixels is weaker,

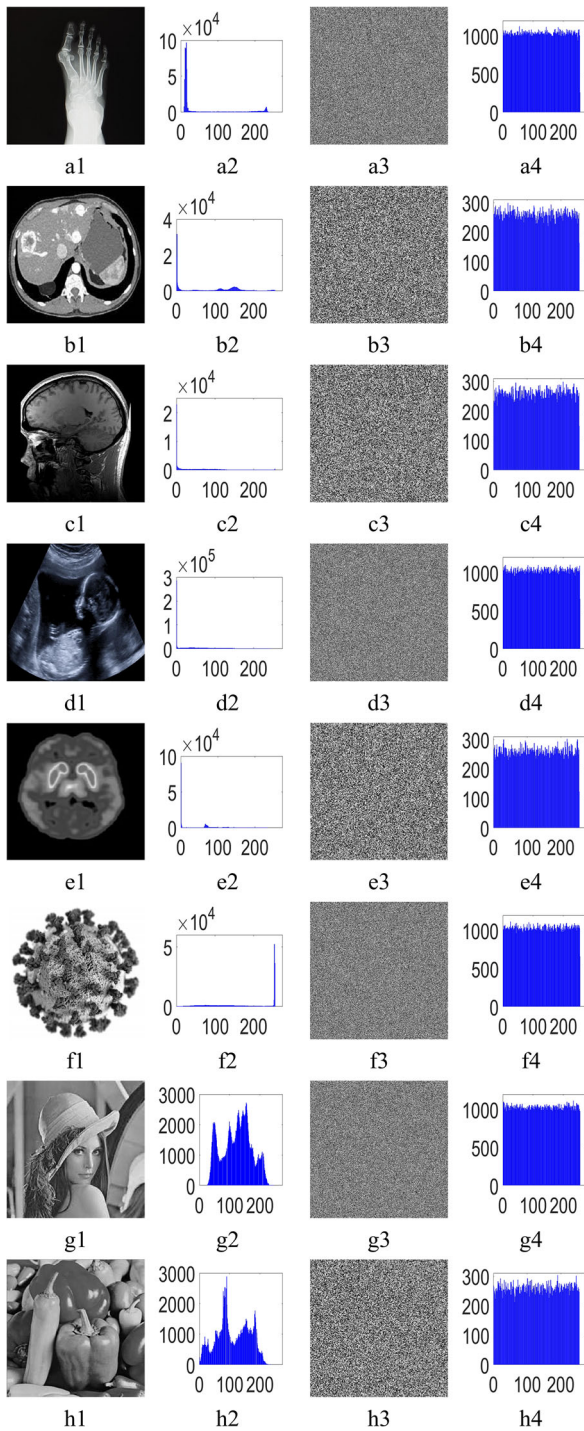


Fig. 7 The histogram of sample images (1st column: plain-image; 2nd column: histogram of plain-image; 3rd column: corresponding cipher-image; 4th column: histogram of cipher-image)

Table 4 The information entropy of sample images

Image ID and type	Color depth	Entropy of plain-image	Entropy of cipher-image
a X-ray	8	4.9130	7.9967
b CT	8	6.5376	7.9969
c MRI	8	5.7123	7.9971
d Ultrasound	8	5.9887	7.9989
e PET	8	4.5179	7.9964
f COVID-19	8	6.4010	7.9989
g Lena	8	7.4455	7.9994
h Peppers	8	7.5631	7.9975

and the security of the encryption algorithm is higher. The correlation of adjacent pixels of plain-images and cipher-images in Fig. 6 is calculated, and the values are listed in Table 5.

It can be seen from the data that the correlation of adjacent pixels of plain-images is strong, while the correlation of adjacent pixels of corresponding cipher-image images is very weak, and the values are close to the ideal value 0. The correlation of adjacent pixels can be illustrated as another intuitive form in Fig. 8 and b. In these figures, it can be easily seen that the correlation of adjacent pixels of plain medical images is strong and its distribution is close to the line of $x = y$, while the correlation of adjacent pixels of corresponding cipher-images is very weak and close to a uniform distribution. Cryptanalysts can hardly get any useful information from the adjacent pixels of the cipher image.

The key analysis **Keyspace analysis** Keyspace is the set of all possible keys in a cryptosystem. The larger the keyspace, the higher the security of the encryption algorithm, and the stronger the ability to resist brute force attacks. In general, the keyspace of a cryptosystem should not be less than 2^{100} [6], which is about 1.27×10^{30} . However, as computing power continues to improve, we recommend that the keyspace should be much larger than 2^{100} .

For chaotic map-based cryptosystems, the range of chaotic control parameters and chaotic initial values are usually the keyspace. For the proposed algorithm, the factors affecting the keyspace are chaotic control parameters a, b and chaotic initial values x_1, y_1 . The computing accuracy used in this paper is 1×10^{-15} , so the key space should be $(1 \times 10^{15})^4$ which is about 2^{200} and large enough to resist brute force attacks. Even with the current world’s fastest computer, the ‘Fugaku’ in Japanese, whose peak computing power is about 5×10^{19} times per second, it will take an average of 4×10^{40} seconds or about 10^{32} years to find the correct key.

Table 5 The correlation of adjacent pixels of sample images

Image ID and type	Plain-image			Cipher-image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
a X-ray	0.994781	0.998650	0.993848	0.002030	-0.003348	0.002698
b CT	0.972369	0.977308	0.956139	-0.004922	-0.002507	0.002236
c MRI	0.935280	0.949021	0.896427	0.007122	0.000747	-0.004353
d Ultrasound	0.991437	0.991388	0.987367	0.001844	0.000342	0.001188
e Pet	0.995131	0.979666	0.975197	-0.010510	-0.001414	-0.003332
f COVID-19	0.985368	0.987217	0.975460	-0.002245	0.000035	-0.000074
g Lena	0.971872	0.984984	0.959273	0.000149	0.001987	0.004100
h Peppers	0.961686	0.967918	0.932524	0.004197	-0.002702	-0.006579

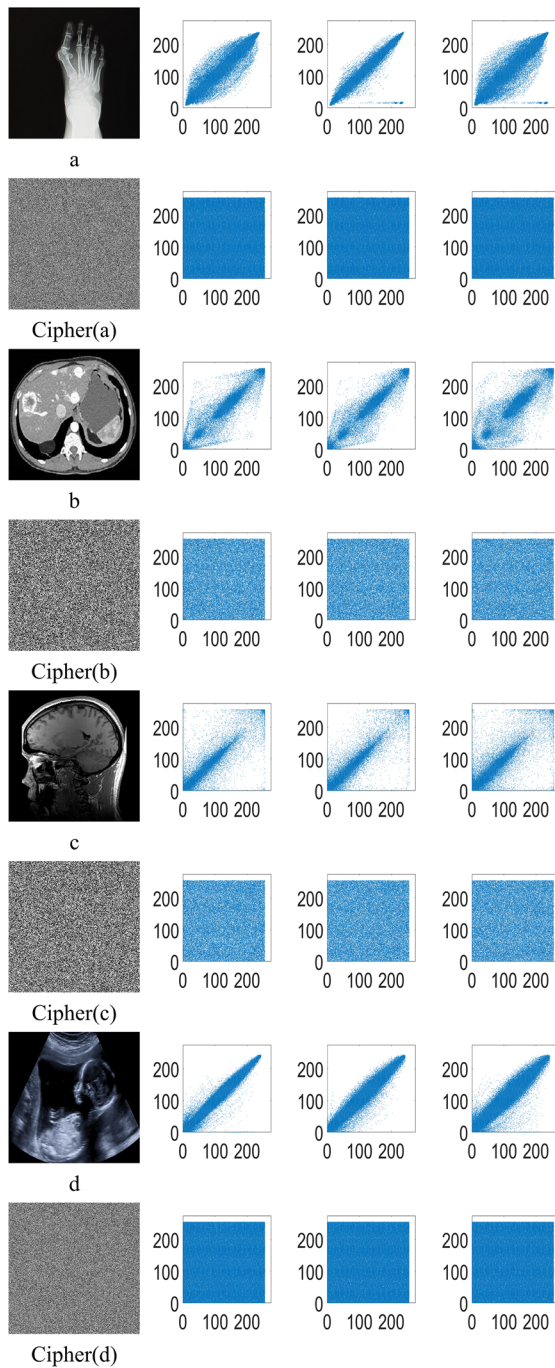


Fig. 8 a. The correlation of sample images a-d in different directions (1st column: plain-images and corresponding cipher-image; 2nd column: correlation diagram in horizontal; 3rd column: correlation diagram in vertical; 4th column: correlation diagram in diagonal). b. The correlation of sample images e-h in different directions (1st column: plain-images and corresponding cipher-image; 2nd column: correlation diagram in horizontal; 3rd column: correlation diagram in vertical; 4th column: correlation diagram in diagonal)

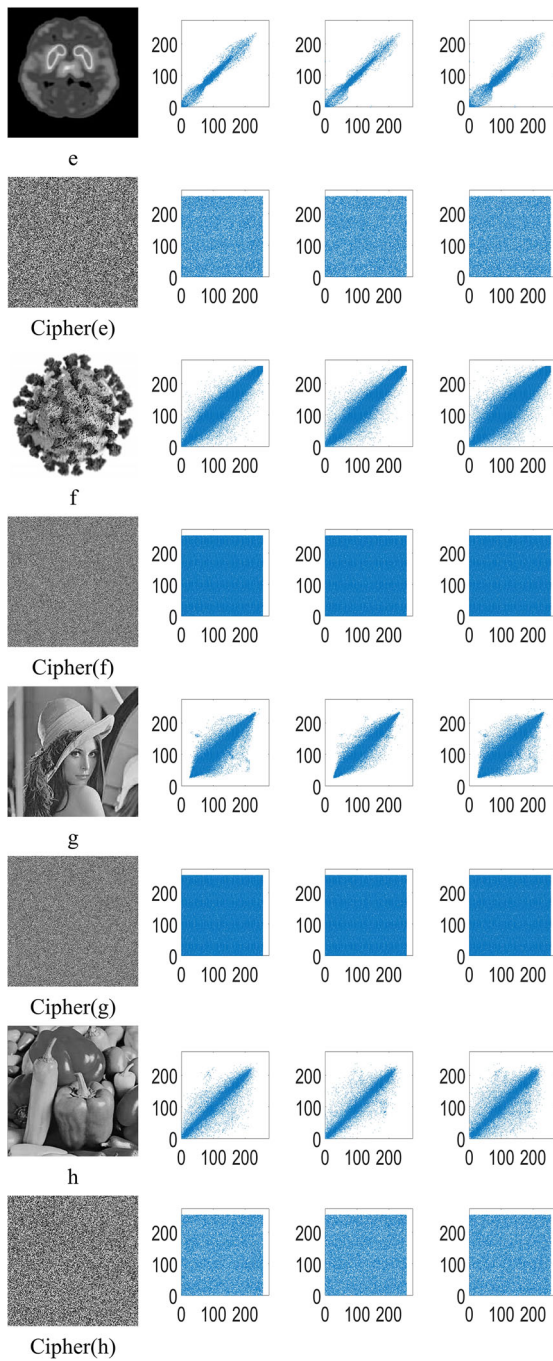


Fig. 8 (continued)

Moreover, the key space of the proposed algorithm has the potential of expansion, which only needs to improve the computing accuracy of the proposed chaotic map.

Key sensitivity analysis The key sensitivity analysis should include two aspects, (1) using two slightly different keys to encrypt the same plain medical image, the corresponding cipher-image will be completely different; (2) using the decryption key, which is slightly different from the encryption key, to decrypt the cipher-image will get a wrong result, and the decryption result should not contain information beyond the cipher-image. Several groups of slightly different chaotic control parameters and chaotic initial values used in key sensitivity analysis are listed in Table 6.

In order to analyze the change degree between the different cipher-image, two quantitative indexes, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI), are used. These two indexes can be calculated as Eq. 6 and Eq. 7, respectively.

$$NPCR = \frac{\sum_{i=1, j=1}^{M, N} D(i, j)}{M \times N} \tag{6}$$

$$UACI = \frac{1}{M \times N} \times \sum_{i=1, j=1}^{M, N} \frac{|I_1(i, j) - I_2(i, j)|}{2^d - 1} \tag{7}$$

Where

$$D(i, j) = \begin{cases} 0 & \text{if } I_1(i, j) = I_2(i, j) \\ 1 & \text{if } I_1(i, j) \neq I_2(i, j) \end{cases} \tag{8}$$

In the Eq. 6, Eq. 7, and Eq. 8:

- M, N is the number of rows and columns of the image respectively.
- d is the color depth of the image I .
- $I_1(i, j)$ is the pixel value of the i row and j column of the image I .
- Σ is the continuous addition symbol.

For two random 8-bit color depth images, the NPCR value should be larger than 0.995693, and the UACI value should be close to 0.334636 [72]. Using the keys in Table 6 to encrypt the examples in Fig. 5, the NPCR and UACI of the results are listed in Tables 7 and 8 respectively.

Table 6 Several groups of slightly different chaotic control parameters and chaotic initial values

Key ID	a	b	x_1	y_1
Original	3.889632578965258	2.895365874521023	0.723657891234568	0.589632147852589
a'	3.889632578965258+ 0.000000000000001	The same	The same	The same
b'	The same	2.895365874521023+ 0.000000000000001	The same	The same
x'_1	The same	The same	0.723657891234568+ 0.000000000000001	The same
y'_1	The same	The same	The same	0.589632147852589+ 0.000000000000001

Table 7 The NPCR value of Key sensitivity analysis

Image ID and size	Changed key	NPCR	Critical values [72]			
			*0.05=0.995693	*0.01=0.995527	*0.001=0.995347	256×256
			*0.05=0.995893	*0.01=0.995810	*0.001=0.995717	512×512
a 512×512	a'	0.996136	Pass	Pass	Pass	
	b'	0.995972	Pass	Pass	Pass	
	x'_1	0.995960	Pass	Pass	Pass	
	y'_1	0.996223	Pass	Pass	Pass	
b 256×256	a'	0.996353	Pass	Pass	Pass	
	b'	0.995758	Pass	Pass	Pass	
	x'_1	0.996231	Pass	Pass	Pass	
	y'_1	0.996078	Pass	Pass	Pass	
c 256×256	a'	0.996277	Pass	Pass	Pass	
	b'	0.995819	Pass	Pass	Pass	
	x'_1	0.995926	Pass	Pass	Pass	
	y'_1	0.995789	Pass	Pass	Pass	
d 512×512	a'	0.997238	Pass	Pass	Pass	
	b'	0.997162	Pass	Pass	Pass	
	x'_1	0.997058	Pass	Pass	Pass	
	y'_1	0.997147	Pass	Pass	Pass	
e 256×256	a'	0.995911	Pass	Pass	Pass	
	b'	0.996216	Pass	Pass	Pass	
	x'_1	0.995834	Pass	Pass	Pass	
	y'_1	0.996155	Pass	Pass	Pass	
f 512×512	a'	0.996750	Pass	Pass	Pass	
	b'	0.996861	Pass	Pass	Pass	
	x'_1	0.996750	Pass	Pass	Pass	
	y'_1	0.996887	Pass	Pass	Pass	
g 512×512	a'	0.996231	Pass	Pass	Pass	
	b'	0.996037	Pass	Pass	Pass	
	x'_1	0.996372	Pass	Pass	Pass	
	y'_1	0.996372	Pass	Pass	Pass	
h 256×256	a'	0.995751	Pass	Pass	Pass	
	b'	0.995880	Pass	Pass	Pass	
	x'_1	0.996063	Pass	Pass	Pass	
	y'_1	0.996124	Pass	Pass	Pass	

It can be seen from the data in these two tables, a slight change in the key will produce completely different encryption results.

The correct decryption results and the incorrect decryption results with slightly different keys for image Fig. 5a are illustrated in Fig. 9, and the statistical indicators of them are analyzed, which are listed in Table 9. The data shows that no useful information can be derived from the incorrect decryption results. The above analysis of encryption and decryption results with slightly different keys shows that the algorithm has good key sensitivity.

Chosen plain-image analysis Differential analysis is a common method of chosen plain-image cryptanalysis, in which the same key is used to encrypt two slightly different plain-image and then compare the corresponding two cipher-images to find useful information. An excellent medical image encryption algorithm should ensure that the NPCR and UACI values are close to the value of the two random images when using the differential attack to analyze it.

Table 8 The UACI value of Key sensitivity analysis

Image ID and size	Changed key	UACI	Critical values [72]		
			*-0.05=0.332824	*-0.01=0.332255	*-0.001=0.331594
			*+0.05=0.336447	*+0.01=0.337016	*+0.001=0.337677
			*-0.05=0.333730	*-0.01=0.333445	*-0.001=0.333115
			*+0.05=0.335541	*+0.01=0.335826	*+0.001=0.336156
a 512×512	a'	0.333749	Pass	Pass	Pass
	b'	0.333877	Pass	Pass	Pass
	x'_1	0.333788	Pass	Pass	Pass
	y'_1	0.333504	Pass	Pass	Pass
b 256×256	a'	0.333648	Pass	Pass	Pass
	b'	0.334666	Pass	Pass	Pass
	x'_1	0.333258	Pass	Pass	Pass
	y'_1	0.333504	Pass	Pass	Pass
c 256×256	a'	0.334623	Pass	Pass	Pass
	b'	0.334442	Pass	Pass	Pass
	x'_1	0.333934	Pass	Pass	Pass
	y'_1	0.334917	Pass	Pass	Pass
d 512×512	a'	0.335067	Pass	Pass	Pass
	b'	0.334352	Pass	Pass	Pass
	x'_1	0.334508	Pass	Pass	Pass
	y'_1	0.334521	Pass	Pass	Pass
e 256×256	a'	0.333669	Pass	Pass	Pass
	b'	0.334881	Pass	Pass	Pass
	x'_1	0.335564	Pass	Pass	Pass
	y'_1	0.333398	Pass	Pass	Pass
f 512×512	a'	0.335360	Pass	Pass	Pass
	b'	0.334900	Pass	Pass	Pass
	x'_1	0.334591	Pass	Pass	Pass
	y'_1	0.334779	Pass	Pass	Pass
g 512×512	a'	0.334721	Pass	Pass	Pass
	b'	0.334888	Pass	Pass	Pass
	x'_1	0.335187	Pass	Pass	Pass
	y'_1	0.335495	Pass	Pass	Pass
h 256×256	a'	0.335523	Pass	Pass	Pass
	b'	0.336434	Pass	Pass	Pass
	x'_1	0.333963	Pass	Pass	Pass
	y'_1	0.333740	Pass	Pass	Pass

Table 9 The statistical indicators of the incorrect decryption results

Image	Correlation of adjacent pixels			Entropy
	horizontal	vertical	diagonal	
a'	-0.000723	0.003149	-0.001526	7.999329
b'	-0.001093	0.002396	-0.002192	7.999270
x'_1	0.001129	-0.000431	-0.001299	7.999258
y'_1	-0.000825	-0.001922	-0.001250	7.999233

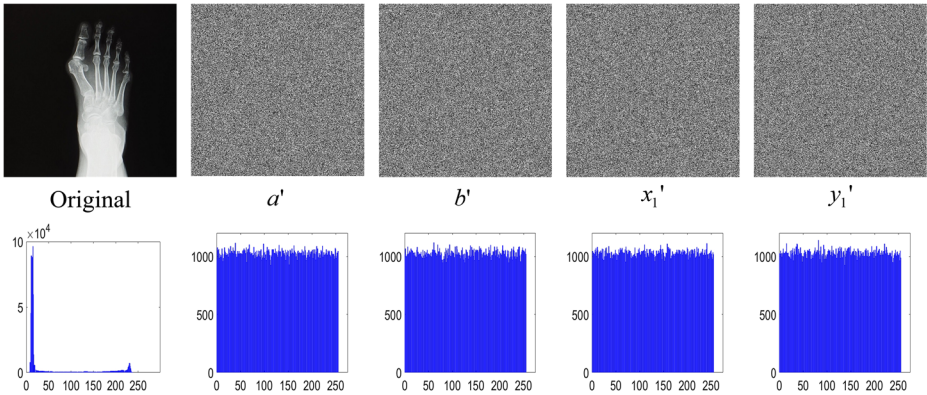


Fig. 9 The correct decryption results and the incorrect decryption results with slightly different keys for image a, as well as their corresponding histograms

For the eight samples in Fig. 5, one pixel was selected randomly, and its value was changed slightly. Then these two slightly different images were encrypted with the same key. The original images, slightly changed images, corresponding encryption results, and the difference between these two sets of encryption results with their histograms are illustrated in Fig. 10. The NPCR and UACI values of these two cipher-image groups are listed in Tables 10 and 11. It can be seen from the data that completely different cipher-image can be obtained even if the plain-image is only changed slightly, and the comparative analysis of the two cipher-images can hardly find any useful information. Therefore, the proposed algorithm can resist the attack of differential analysis.

Black and white image analysis Black and white image analysis is another commonly used method of chosen plain-image cryptanalysis, which is often used to try to obtain the encryption key of the substitution phase. The visual quality and histogram analysis of cipher black and white images is shown in Fig. 11. It can be seen from the figure that the cipher-images visual quality is good, and the corresponding histograms distribute uniformly. Table 12 shows part of the quantitative analysis results of the black and white image analysis. The results show that the correlation between adjacent pixels of cipher-image is low, and its information entropy is close to the theoretical upper limit.

Since the black and white images have no medical visual significance, the whole image is divided into ROB. So there isn't any permutation was performed, and only the substitution was performed to encrypt black and white images. The cipher-image is the encryption key of the substitution phase. However, it is not feasible to crack the encryption results of other images only through the substitution key of black and white images. The first reason is that there is no feasible method to obtain the key generation key, which is chaotic initial values and chaotic parameters, from the substitution key. This was because of the introduction of the 'mod' operations in the encryption key generation phase. The second reason is that the encryption key is plain-image correlative. Even if the same key generation key is used to encrypt different images, different encryption keys will be generated in the process.

The results of differential analysis and black and white images analysis show that the proposed algorithm has the ability to resist chosen plain-image attacks.

Fig. 10 Slightly different plain image, corresponding cipher-image, and the different between them (1st column: original plain-images; 2nd column: slightly changed images; 3rd column: cipher-images of original; 4th column: cipher-images of slightly changed images; 5th column: The difference between two sets of cipher-images; 6th column: histogram of the difference between two sets of cipher-images)

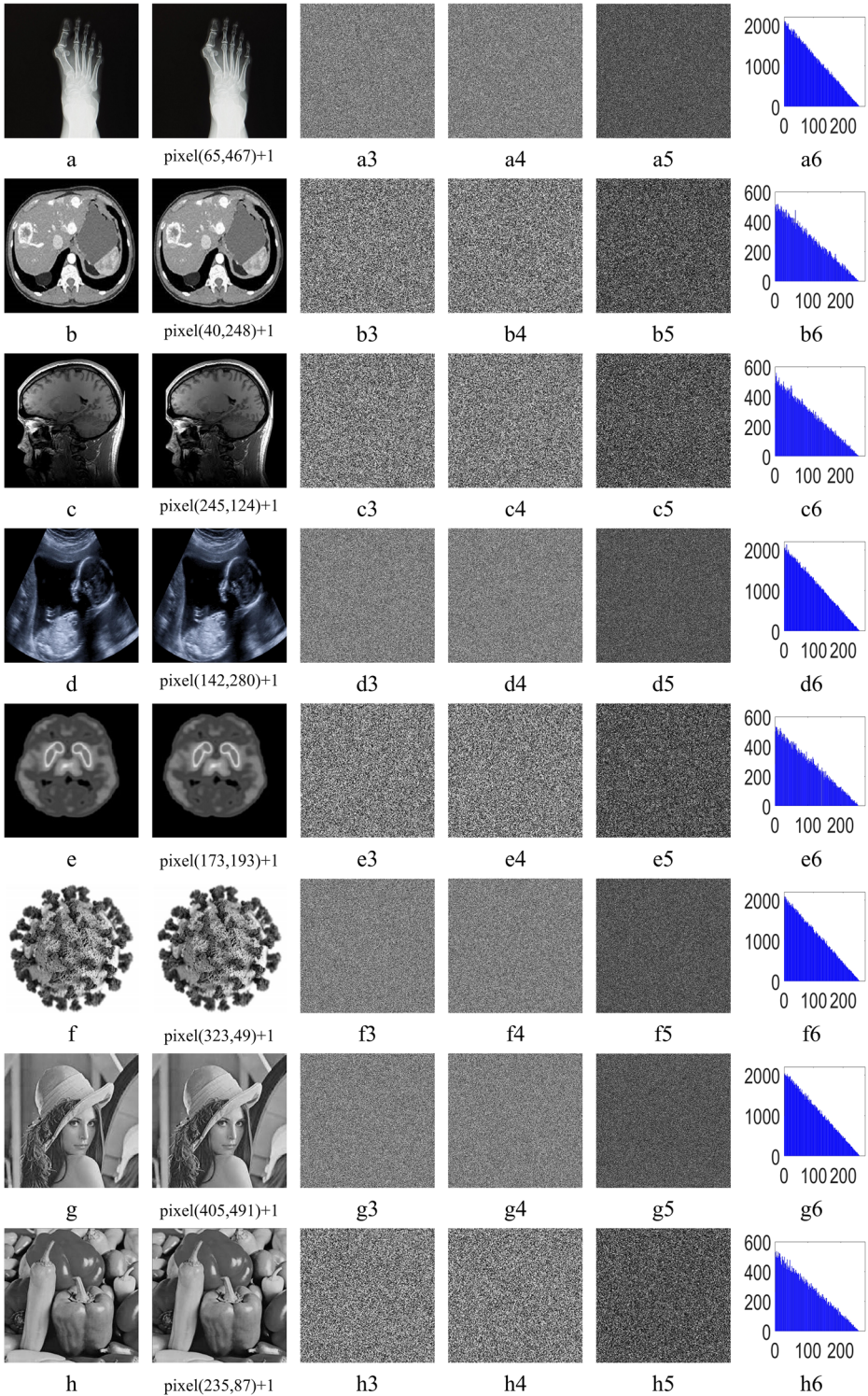


Table 10 The NPCR values of differential analysis

Image ID and size	NPCR	Critical values [72]			
		*0.05=0.995693 *0.05=0.995893	*0.01=0.995527 *0.01=0.995810	*0.001=0.995347 *0.001=0.995717	256 × 256 512 × 512
a 512 × 512	0.996361	Pass	Pass	Pass	
b 256 × 256	0.996109	Pass	Pass	Pass	
c 256 × 256	0.996124	Pass	Pass	Pass	
d 512 × 512	0.996197	Pass	Pass	Pass	
e 256 × 256	0.996033	Pass	Pass	Pass	
f 512 × 512	0.996113	Pass	Pass	Pass	
g 512 × 512	0.996063	Pass	Pass	Pass	
h 256 × 256	0.996399	Pass	Pass	Pass	

4.2.2 Time complexity analysis

The proposed encryption algorithm consists of the key generation stage and the image encryption stage. In the key generation stage, the time complexity of generating chaotic sequences with $M \times N$ length is $O(MN)$. Since only the ROI of medical images need to be permuted, the key length is smaller than $M \times N$, so the time complexity of generating the key for permutation is less than $O(MN \log_2(MN))$. At the same time, the time complexity of generating the key for substitution is $O(MN)$. Therefore, the time complexity of the key generation stage is less than $O(MN \log_2(MN))$. In the image encryption stage, pixel permutation and substitution are both linear operations, in which the time complexity of permutation is less than $O(MN)$ and the time complexity of substitution is $O(MN)$, so the time complexity of the encryption stage is less than $O(2MN)$.

The proposed algorithm was simulated and the actual running time was measured. The results are listed in Table 13. As can be seen from the table, for images of the same size, the permutation and overall encryption speed of medical images are significantly faster than that of normal images due to the reduction of the amount of data permuted.

Table 11 The UACI values of differential analysis

Image ID and size	UACI	Critical values [72]			
		*-0.05=0.332824 *+0.05=0.336447 *-0.05=0.333730 *+0.05=0.335541	*-0.01=0.332255 *+0.01=0.337016 *-0.01=0.333445 *+0.01=0.335826	*-0.001=0.331594 *+0.001=0.337677 *-0.001=0.333115 *+0.001=0.336156	256 × 256 512 × 512
a 512 × 512	0.333782	Pass	Pass	Pass	
b 256 × 256	0.333385	Pass	Pass	Pass	
c 256 × 256	0.334302	Pass	Pass	Pass	
d 512 × 512	0.333965	Pass	Pass	Pass	
e 256 × 256	0.332984	Pass	Pass	Pass	
f 512 × 512	0.334728	Pass	Pass	Pass	
g 512 × 512	0.335461	Pass	Pass	Pass	
h 256 × 256	0.333319	Pass	Pass	Pass	

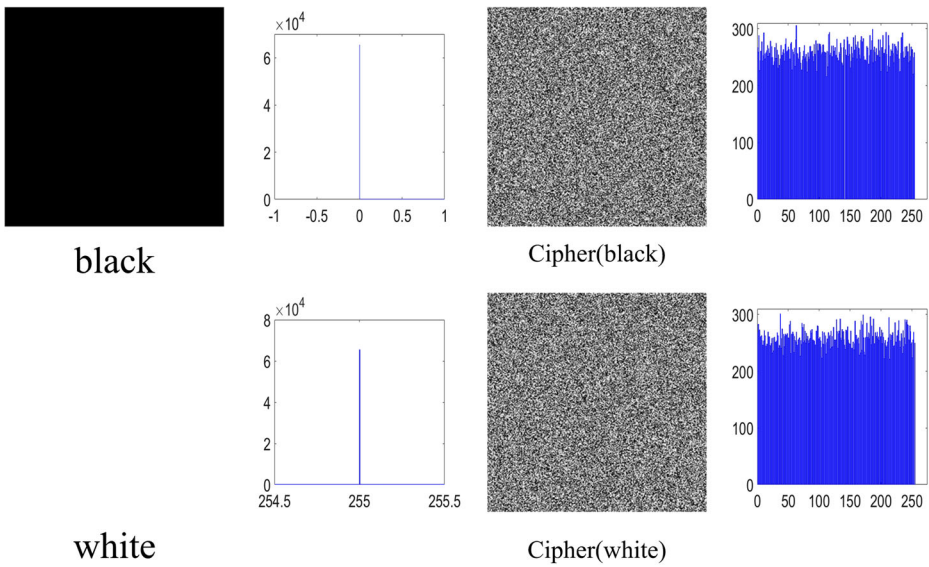


Fig. 11 Black and white image encryption results and histogram analysis (1st column: original black and white images; 2nd column: Histograms of black and white images; 3rd column: cipher black and white images; 4th column: Histograms of cipher-images)

Table 12 The statistical indicators of the black and white image

Image		Correlation of adjacent pixels			Entropy
		horizontal	vertical	diagonal	
Plain-image	Black	1.000000	1.000000	1.000000	0.0000
	White	1.000000	1.000000	1.000000	0.0000
Cipher-image	Black	0.001316	-0.002754	-0.002355	7.9922
	White	-0.003170	-0.000321	-0.000158	7.9914

Table 13 The actual running time and throughput of samples

Image	Ratio of ROI	Encryption time			Decryption time	Throughput
		Permutation	Substitution	Total		
a X-ray	26%	0.171 s	0.344 s	0.515 s	0.749 s	3.88Mbps
b CT	72%	0.134 s	0.203 s	0.337 s	0.512 s	1.48 Mbps
c MRI	63%	0.164 s	0.215 s	0.379 s	0.506 s	1.48 Mbps
d Ultrasound	71%	0.252 s	0.376 s	0.628 s	0.604 s	3.79 Mbps
e Pet	48%	0.151 s	0.201 s	0.352 s	0.507 s	1.42 Mbps
f COVID-19	65%	0.210 s	0.346 s	0.556 s	0.596 s	3.60Mbps
g Lena	100%	0.323 s	0.365 s	0.687 s	0.751 s	2.91 Mbps
h Peppers	100%	0.262 s	0.219 s	0.481 s	0.513 s	1.04 Mbps

Table 14 The cipher-image visual quality comparative analyses

Literature	Method	Cipher-Image Visual Quality
[3, 78]	Only the LL sub-band of the image transform domain is encrypted.	Poor, the more times transformation, the worse the cipher-image quality.
[52, 59]	Only the selected rectangular region in the center of medical image is encrypted.	Poor, there is no protection outside the rectangular region.
[34, 51]	Only the ROI of medical image is encrypted.	Poor, ROB is not encrypted and the shape of ROI can be easily seen.
[36]	Only the edge map of medical image is encrypted.	Poor, the region outside the edge map is not being protected.
[46, 50]	The selective region is substituted first, and then the whole image is permuted.	Good, but did not change the statistical characteristics of the non-selected region.
[21, 48]	High information bit-planes are permuted first, and then the whole image is substituted.	Very good
[4]	The selective region is permuted first, and then the whole image is substituted.	Very good
[63]	Three level encryption. Permute high information 4 bit-planes, substitute the LL sub-band of the transform domain, permute high information 4 bit-planes.	Very good
[45]	Three level encryption. Full encryption, using RC6 to encrypt the LL sub-band of the transform domain, full encryption.	Very good
Proposed	The selective region is permuted first, and then the whole image is substituted.	Very good

4.3 Comparative analysis

The proposed algorithm is compared with some methods discussed in the literature review of Section 1. The cipher-image visual quality comparative analyses are shown in Table 14. It can be seen from the table that the cipher-image visual quality of the proposed semi-selective encryption algorithm is better than that of full-selective encryption algorithms. Some main quantitative index values of the proposed algorithm are compared with other semi-selective encryption algorithms, and the results are listed in Table 15. It can be seen that the proposed algorithm is superior to or at least not worse than the existing method in all major indicators.

Table 15 Some main quantitative index values comparative analysis (Bold italics: not ideal value)

Literature	Average correlation between adjacent pixels	Average NPCR	Average UACI	Average entropy	Key space	Time complexity	
						O()	Throughput
[50]	NA	0.9961	0.3346	7.1730	NA	NA	
[48]	0.001757	0.9998	0.3347	7.9998	$\approx 2^{300}$	O(2MN)	1.75Mbps
[63]	NA	0.9965	0.3361	7.9983	2^{135}	<O(3MN)	620Kbps
[45]	0.028	0.9962	0.3346	7.9990	2^{1500}	>O(4MN)	52 Kbps
[21]	0.002196	0.9986	0.3316	NA	2^{57}	> O(300MN)	
[4]	0.019933	0.9987	0.3329	7.846	2^{399}	O(4MN)	
Proposed	0.002778	0.9962	0.3337	7.9974	2^{200}	<O(2MN)	2.45Mbps

5 Conclusion

In this work, an enhanced 2D-Logistic chaotic map was designed, in which the number of chaotic control parameters and chaotic initial values was increased, the value range of chaotic control parameters was expanded, and the chaotic windows were eliminated, when compared with the original 1-D Logistic map. Then, based on the characteristics that medical images can be divided into ROI and ROB, a plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-Logistic map was proposed. The simulation results analysis showed that the algorithm has good security and high encryption speed. Therefore, it is suitable to protect the confidentiality of medical images. The future recommended work is to combine the semi-selective image encryption structure with other high-information region segmentation methods, such as bit-plane segmentation or transform domain. Another suggested research direction is to explore the implementation of the algorithm on different medical platforms.

Declarations No conflicts of interest, all medical image samples are obtained from open sources and do not involve the patient's privacy.

References

1. Aashiq Banu S, Amirtharajan R (2020) A robust medical image encryption in dual domain : chaos-DNA-IWT combined approach. *Med Biol Eng Comput* 58(7):1445–1458
2. Abd El-Latif AA, Abd-El-Atty B, Talha M (2017) Robust encryption of quantum medical images. *IEEE Access* 6:1073–1081. <https://doi.org/10.1109/ACCESS.2017.2777869>
3. Abdmouleh, M. K., Khalfallah, A., & Bouhlel, M. S. (2017). A novel selective encryption DWT-based algorithm for medical images. 2017 14th international conference on computer graphics, imaging and visualization, 79–84. <https://doi.org/10.1109/CGIV.2017.10>
4. Akkasaligar PT, Biradar S (2020) Selective medical image encryption using DNA cryptography. *Inf Sec J: A Global Persp* 29(2):91–101. <https://doi.org/10.1080/19393555.2020.1718248>
5. Al-haj A, Abandah G, Hussein N (2015) Crypto-based algorithms for secured medical image transmission. *IET Inf Secur* 9(6):365–373. <https://doi.org/10.1049/iet-ifs.2014.0245>
6. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int J Bifurcation Chaos* 16(08):2129–2151
7. Arumugham S, Rajagopalan S, Bosco J, Rayappan B, Amirtharajan R (2018) Networked medical data sharing on secure medium—A web publishing mode for DICOM viewer with three layer authentication. *J Biomed Inform* 86:90–105. <https://doi.org/10.1016/j.jbi.2018.08.010>
8. Arunkumar S, Subramaniaswamy V, Vijayakumar V, Chilamkurti N, Logesh R (2019) SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement* 139:426–437. <https://doi.org/10.1016/j.measurement.2019.02.069>
9. Bakshi A, Patel AK (2019) Secure telemedicine using RONI halftoned visual cryptography without pixel expansion. *J Inf Sec Appl* 46:281–295. <https://doi.org/10.1016/j.jisa.2019.03.004>
10. Balasamy K, Suganyadevi S (2021) A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed Tools Appl* 80:7167–7186
11. Banik A, Shamsi Z, Laiphrakpam DS (2019) An encryption scheme for securing multiple medical images. *J Inf Sec Appl* 49:102398. <https://doi.org/10.1016/j.jisa.2019.102398>
12. Barik RC, Changder S (2021) A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps. *Multimed Tools Appl* 80:10723–10760
13. Belazi A, Talha M, Kharbech S, Xiang W (2019) Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access* 7:36667–36681. <https://doi.org/10.1109/ACCESS.2019.2906292>
14. Chandrasekaran J, Thiruvengadam SJ (2017) A hybrid chaotic and number theoretic approach for securing DICOM images. *Sec Comm Networks* 2017:1–12

15. Chen M, Ma G, Tang C, Lei Z (2020) Generalized optical encryption framework based on Shearlets for medical image. *Opt Lasers Eng* 128:106026. <https://doi.org/10.1016/j.optlaseng.2020.106026>
16. Chen X, Hu C (2017) Adaptive medical image encryption algorithm based on multiple chaotic mapping. *Saudi J Biol Sci* 24(8):1821–1827. <https://doi.org/10.1016/j.sjbs.2017.11.023>
17. Chen X, Hu C-J (2017) Medical image encryption based on multiple chaotic mapping and wavelet transform. *Biomed Res* 28(20):8834–8837
18. Chirakkarottu S, Mathew S (2020) A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography. *SN Appl Sci* 2(1):1–10. <https://doi.org/10.1007/s42452-019-1685-8>
19. *Cryptography Law*, (2019).
20. Dagadu JC, Li J, Aboagye EO (2019) Medical image encryption based on hybrid chaotic DNA diffusion. *Wirel Pers Commun* 108(1):591–612. <https://doi.org/10.1007/s11277-019-06420-z>
21. Dai Y, Wang H, Wang Y (2016) Chaotic medical image encryption algorithm based on bit-plane decomposition. *Int J Pattern Recognit Artif Intell* 30(4):1657001. <https://doi.org/10.1142/S0218001416570019>
22. Dai Y, Wang H, Zhou Z, Jin Z (2016) Research on medical image encryption in telemedicine systems. *Technol Health Care* 24(s2):S435–S442. <https://doi.org/10.3233/THC-161166>
23. Devi RS, Thenmozhi K, Rayappan JBB, Amirtharajan R, Praveenkumar P (2019) Entropy influenced RNA diffused quantum chaos to conserve medical data privacy. *Int J Theor Phys* 56(6):1937–1956
24. Dridi M, Hajjaji MA, Bouallegue B, Mtibaa A (2016) Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Process* 10(11):830–839. <https://doi.org/10.1049/iet-ipr.2015.0868>
25. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurcation Chaos* 8(06):1259–1284
26. Gafsi M, Abbassi N, Hajjaji MA, Malek J, Mtibaa A (2020) Improved chaos-based cryptosystem for medical image encryption and decryption *Sci Prog* 2020
27. Ge J (2020) Alccryption : A secure and efficient algorithm for medical. *IEEE Signal Process Lett* 125(3):1083–1100. <https://doi.org/10.32604/cmes.2020.013039>
28. Gupta R, Pachauri R, Singh AK (2018) An effective approach of secured medical image transmission using encryption method. *Mole Cell Biomech* 15(2):63. <https://doi.org/10.3970/mcb.2018.00114>
29. Hua Z, Yi S, Zhou Y (2018) Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process* 144:134–144. <https://doi.org/10.1016/j.sigpro.2017.10.004>
30. Ismail SM, Said LA, Radwan AG, Madian AH, Abu-elyazeed MF (2018) Generalized double-humped logistic map-based medical image encryption. *J Advan Res* 10:85–98. <https://doi.org/10.1016/j.jare.2018.01.009>
31. Jain M, Choudhary RC, Kumar A (2016) Secure medical image steganography with RSA cryptography using decision tree. In: 2016 2nd international conference on contemporary computing and informatics (IC3I), pp 291–295. <https://doi.org/10.1109/IC3I.2016.7917977>
32. Jiao G, Peng X, Duan K (2019) Image encryption with the cross diffusion of two chaotic maps. *KSII Trans Int Inform Syst (TIIS)* 13(2):1064–1079
33. Jiao G, Zhou S, Li L, Zou Y (2019) Hybrid chaotic encryption algorithm for securing dicom systems. *Int J Perform Eng* 15(5):1436–1444. <https://doi.org/10.23940/ijpe.19.05.p20.14361444>
34. Kanso A, Ghebleh M (2015) An efficient and robust image encryption scheme for medical applications. *Commun Nonlinear Sci Numer Simul* 24(1–3):98–116. <https://doi.org/10.1016/j.cnsns.2014.12.005>
35. Kanso A, Ghebleh M (2018) An efficient lossless secret sharing scheme for medical images. *J Vis Commun Image Represent* 56:245–255. <https://doi.org/10.1016/j.jvcir.2018.09.018>
36. Khashan OA, Alshaikh M (2020) Edge-based lightweight selective encryption scheme for digital medical images. *Multimed Tools Appl* 79(35):26369–26388
37. Khond S, Vijayakumar B (2019) Secure medical image processing using chaos and DNA encryption enhanced using reversible data hiding. *Int J Eng Adv Technol (IJEAT)* 8(6S):1062–1067. <https://doi.org/10.35940/ijeat.F1202.0886S19>
38. Koppu S, Viswanatham VM (2018) Medical image security enhancement using two dimensional chaotic mapping optimized by self-adaptive grey wolf algorithm. *Evol Intel* 11(1):53–71. <https://doi.org/10.1007/s12065-018-0159-z>
39. Kumar CV, Natarajan V, Poonguzhali P (2015) Secured patient information transmission using reversible watermarking and DNA Encryption for medical images. *Appl Math Sci* 9(48):2381–2391
40. Kumar S, Panna B, Kumar R (2019) Medical image encryption using fractional discrete cosine transform with chaotic function. *Med Biol Eng Comput* 57(11):2517–2533
41. Lakshmi C, Thenmozhi K, Rayappan JBB, Rajagopalan S, Amirtharajan R, Chidambaram N (2020) Neural-assisted image-dependent encryption scheme for medical image cloud storage. *Neural Comput Appl* 33:9–6684. <https://doi.org/10.1007/s00521-020-05447-9>

42. Liu J, Ma Y, Li S, Lian J, Zhang X (2018) A new simple chaotic system and its application in medical image encryption. *Multimed Tools Appl* 77(17):22787–22808
43. Liu J, Li J, Cheng J, Ma J, Sadiq N, Han B, Geng Q, Ai Y (2019) A novel robust watermarking algorithm for encrypted medical image based on DTCWT-DCT and chaotic map. *Comput, Mat Continua* 61(2):889–910. <https://doi.org/10.32604/cmc.2019.06034>
44. Madhusudhan K, Sakthivel P (2020) A secure medical image transmission algorithm based on binary bits and Arnold map. *J Ambient Intell Human Comp*:1–8. <https://doi.org/10.1007/s12652-020-02028-5>
45. Manikandan V, Amirtharajan R (2021) On dual encryption with RC6 and combined logistic tent map for grayscale and DICOM. *Multimed Tools Appl* 80(15):23511–23540
46. Manikandan V, Amirtharajan R (2022). A simple embed over encryption scheme for DICOM images using Bülban Map. *Med Biol Eng Comput*, 1–17. <https://doi.org/10.1007/s11517-021-02499-4>
47. Mortajez S, Tahmasbi M, Zarei J, Jamshidnezhad A (2020) A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images. *Inform Med Unlocked* 20: 100396. <https://doi.org/10.1016/j.imu.2020.100396>
48. Muthu JS, Murali P (2022) A novel DICOM image encryption with JSMP map. *Optik* 251(2022):168416. <https://doi.org/10.1016/j.ijleo.2021.168416>
49. Norcen R, Podesser M, Pommer A, Schmidt H-P, Uhl A (2003) Confidential storage and transmission of medical image data. *Comput Biol Med* 33(3):277–292. [https://doi.org/10.1016/S0010-4825\(02\)00094-X](https://doi.org/10.1016/S0010-4825(02)00094-X)
50. Noura M, Noura H, Chehab A, Mansour MM, Sleem L, Couturier R (2018) A dynamic approach for a lightweight and secure cipher for medical images. *Multimed Tools Appl* 77(23):31397–31426
51. Ping P, Zhang X, Yang X, Abdelsattar Y, Hashems A (2022) A novel medical image encryption based on cellular automata with ROI position embedded. *Mult Tools Appl*:1–21
52. Prabhavathi K, Sathisha C, Ravikumara K (2017). Region of interest based selective medical image encryption using multi chaotic system. 2017 international conference on electrical, electronics, communication, computer, and optimization techniques (ICECCOT), 1–5
53. Praveenkumar P, Devi NK, Ravichandran D, Avila J, Thenmozhi K, Rayappan JBB, Amirtharajan R (2018) Transreceiving of encrypted medical image-a cognitive approach. *Multimed Tools Appl* 77(7):8393–8418. <https://doi.org/10.1007/s11042-017-4741-7>
54. Qasim KR, Qasim SS (2020) Encrypt medical image using Csalsa20 stream algorithm. *Medico-Legal Update* 20(3):1248–1256
55. Rahmatullah B, Besar R (2007) Comparison of morphological-based segmentation methods for fetal femur length measurements. *J Mech Med Biol* 7(03):247–263
56. Rahmatullah B, Noble JA (2013) Anatomical object detection in fetal ultrasound: computer-expert agreements. *Int Conf Biom Inf Technol*:207–218
57. Raja S (2019) Multiscale transform-based secured joint efficient medical image compression-encryption using symmetric key cryptography and ebct encoding technique. *Int J Wavelets, Multiresolution Inform Process* 17(05):1950034. <https://doi.org/10.1142/S0219691319500346>
58. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R (2016) Chaos based crossover and mutation for securing DICOM image. *Comput Biol Med* 72:170–184. <https://doi.org/10.1016/j.cmpbiomed.2016.03.020>
59. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R (2017) DNA chaos blend to secure medical privacy. *IEEE Trans Nanobiosci* 16(8):850–858
60. Ravichandran D, Aashiq Banu S, Murthy BK, Balasubramanian V, Fathima S, Amirtharajan R (2021) An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Med Biol Eng Comput* 59(3):589–605
61. Sangavi V, Thangavel P (2020) An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and sine map. *J Inform Secur Appl* 55:102626. <https://doi.org/10.1016/j.jisa.2020.102626>
62. Sasikaladevi N, Geetha K, Revathi A (2019) EMOTE – multilayered encryption system for protecting medical images based on binary curve. *J King Saud Univ - Comput Inform Sci* 32(10):1215. <https://doi.org/10.1016/j.jksuci.2019.01.014>
63. Shafique A, Ahmed J, Rehman MUR, Hazzazi MM (2021) Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain. *IEEE Access* 9:59108–59130. <https://doi.org/10.1109/ACCESS.2021.3071535>
64. Shahzadi R, Anwar SM, Qamar F, Ali M, Rodrigues JJPC (2019) Chaos based enhanced RC5 algorithm for security and integrity of clinical images in remote health monitoring. *IEEE Access* 7:52858–52870. <https://doi.org/10.1109/ACCESS.2019.2909554>
65. Shankar K, Elhoseny M, Dhiravida E, Lakshmanprabu SK, Wu W (2018) An efficient optimal key based chaos function for medical image security. *IEEE Access* 6:77145–77154. <https://doi.org/10.1109/ACCESS.2018.2874026>

66. Singh LD, Singh KM (2017) Medical image encryption based on improved ElGamal encryption technique. *Optik - Int J Light Electron Optics* 147:88–102. <https://doi.org/10.1016/j.ijleo.2017.08.028>
67. Stalin S, Maheshwary P, Shukla PK, Maheshwari M, Gour B, Khare A (2019) Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA). *J Med Syst* 43(8):267
68. Tamilselvi R, Ravindran G (2015) Comparison of encryption efficiency in DICOM images based on radon and block transform. *Int J ChemTech Res* 8(6):843–846
69. Tamrin KF, Rahmatullah B, Samuri SM (2015) Aberration compensation of holographic particle images using digital holographic microscopy. *J Mod Opt* 62(9):701–711. <https://doi.org/10.1080/09500340.2014.1003257>
70. The Health insurance portability and accountability act, (1996).
71. Weijia C, Yicong Z, Philip CLC, Liming, X. (2017) Medical image encryption using edge maps. *Signal Process* 132:96–109. <https://doi.org/10.1016/j.sigpro.2016.10.003>
72. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology. J Selected Areas Telecommun (JSAT)* 1(2):31–38
73. Yang Y, Xiao X, Cai X, Zhang W (2019) A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access* 7:96900–96911
74. Ye C, Xiong Z, Ding Y, Zhang X, Wang G, Xu F (2015) Joint fingerprinting/encryption for medical image security. *Int J Sec Appl* 9(1):409–418
75. Zhang B, Rahmatullah B, Wang SL, Zaidan A, Zaidan B, Liu P (2020) A review of research on medical image confidentiality related technology coherent taxonomy , motivations , open challenges and recommendations. *Multimedia Tools Appl*:1–40
76. Zhang L, Zhu Z, Yang B, Liu W, Zhu H, Zou M (2015) Cryptanalysis and improvement of an efficient and secure medical image protection scheme. *Math Probl Eng* 2015:1–11
77. Zhang L, Zhu Z, Yang B, Liu W, Zhu H, Zou M (2015) Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. *Math Probl Eng* 2015:2015–2019
78. Zhou J, Li J, Di X (2020) A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. *IEEE Access* 8:122210–122228. <https://doi.org/10.1109/ACCESS.2020.3007550>

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.