IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 22, 2020, accepted July 2, 2020, date of publication July 6, 2020, date of current version July 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007550

A Novel Lossless Medical Image Encryption Scheme Based on Game Theory With Optimized ROI Parameters and Hidden ROI Position

JIAN ZHOU[1,2], JINQING LI[1,2], AND XIAOQIANG DI[1,2,3]

[1]School of Computer Science and Technology, Changchun University of Science and Technology, Changchun 130022, China
[2]Jilin Province Key Laboratory of Network and Information Security, Changchun 130033, China
[3]Information Center, Changchun University of Science and Technology, Changchun 130022, China

Corresponding author: Jinqing Li (lijinqing@cust.edu.cn)

This work was supported in part by the Natural Science Foundation Project of the Science and Technology Department, Jilin Province, under Grant 20190201188JC, in part by the Higher Education Teaching Reform Research Project of the Education Department, Jilin Province, under Grant JLLG68552019072509300 4, and in part by the Educational Science Planning Project of the Education Department, Jilin Province, under Grant 20181219140301.

ABSTRACT Medical images contain a large amount of patients' private information. The theft and destruction of medical images will cause irreparable losses to patients and medical institutions. In order to detect the region of interest(ROI) accurately, avoid leakage of ROI position information, and realize lossless recovery of transform domain encryption, we propose a novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. In the encryption process, the ROI is a pixel-level transformed to achieve the lossless decryption of medical images and protect medical image information from loss. At the same time, the position information of the ROI is effectively hidden, and leakage of the position information during transmission is avoided. In addition, the quantum cell neural network(QCNN) hyperchaotic system generates random sequence to scramble and diffuse the ROI. Most important of all, the quantitative analysis method of ROI parameters is given, and the optimal balance between encryption speed and encryption security performance is achieved by using game theory. Simulation experiments and numerical analysis verify that the scheme achieves optimized and lossless encryption and decryption of images, and can flexibly and reliably protect the medical images of different types and structures against various attacks.

INDEX TERMS Game theory, lossless decryption, medical image encryption, quantum cell neural network, region of interest, selective image encryption.

I. INTRODUCTION

With the rapid development of information and network technology, vast amounts of information are transmitted over networks, therefore, information security has received widespread attention [1]–[3]. Digital image possessed the characteristics of intuition and vividness becomes one of the important forms of multimedia information and is widely spread on the Internet along [4]. For certain special fields, such as military, commercial, and medical, digital images usually have higher confidentiality requirements. At present, digital medical images mainly include computed tomography(CT) images, magnetic resonance imaging(MRI) images, B-scan images, digital X-ray machine images, and so on. Digital medical images embed a variety of patient privacy information, and the medical information contained in digital medical images is essential for diagnosis. The leakage and destruction of medical information due to improper protection will cause huge losses and injuries to medical institutions and patients, and even pose a threat to health and life. With the development of telemedicine technology, medical images need to be stored and transmitted on public channels (such as the Internet), so they are vulnerable to security threats. In order to ensure the privacy and confidentiality of medical images, medical institutions use various security services. Among them, the use of encryption algorithms to protect medical information and resist various types of attacks has become one of the most important technical means [5].

The associate editor coordinating the review of this manuscript and approving it for publication was Sun Junwei.

Many scholars have pointed out that, the image's huge volume and redundancy compared to text data, most of the number theory or algebraic concepts based traditional ciphers appear not to be ideal for digital image [6]. The past two decades have seen the rapid development of image encryption and its analysis. Image encryption technology follows the two basic design principles of scrambling and diffusion. At present, according to the encryption method, the image encryption algorithm mainly includes two types, one is full image encryption, which encrypts the whole image, and the other is selective image encryption, which chooses a part of the image for image encryption.

In general, only part of the content in an image is meaningful, that is to say, only part of the image information needs to be encrypted and protected. Therefore, the image is divided into two parts, namely the privacy area, also known as the ROI and the privacy-free area, also known as the region of background(ROB) [7]. It is apparent that encrypt the region of interest can not only protect the information but also save computational resources and improve encryption speed, compared with whole image encryption schemes. Generally speaking, the full encryption scheme requires more calculation, lower calculation speed, and higher requirements on the equipment. However, in wireless medical networks and mobile medical services, information processing requires timely, mobile medical equipment and wireless network equipment have limited computing power and are constrained by electrical energy reserves. So traditional full encryption schemes are not suitable for medical image encryption [8].

In the region of interest encryption schemes, how to choose the region of interest is as important as the encryption algorithm. According to the method of privacy region selection, ROI encryption schemes can be classified into two categories: manual selection encryption and automatic selection encryption. The encryption method of manually selecting the ROI means that the user can determine the specific privacy area and then encrypt the selected area [9], [10]. Obviously, the manual selection method is time-consuming and inaccurate. As a result, many automatic selection schemes have been proposed. In [11], it held that the ROI is taken as a square in the middle of medical images, but this method is limited by the shape and size of the ROI and cannot protect private information well. Literature [12] proposed a block-energy-based algorithm is to determine the ROI of the original medical image. After that, the ROI of medical images are encrypted with hyperchaotic systems. A threshold segmentation method based on the average and the standard deviation is designed in [13]. In 2016, Al-Dmour introduced a simple edge detection method to choose the region of interest [14]. In [15], it proposed scheme utilizes salient object detection to automatically, adaptively, and accurately detect the privacy region of a given plain image, the private pixels are encrypted using chaotic cryptography. Artificial neural networks (ANN) are applied to the detection of regions of interest (ROI), and a kind of solution for automatically selecting ROI regions is given in [16]. There are other excellent solutions to choose the privacy regions automatically, such as threshold segmentation, face detection, infrared targeting, and salient mapping [8], [17], [18]. However, most of the above schemes are affected by the fixed segmentation threshold and the fixed detection parameters, and cannot automatically adapt to the images with different structures and formats. Therefore, it is necessary to further study and design an automatic ROI selection method that can automatically adapt to different formats and types of images, to accurately and effectively select ROI quickly.

In the selective image encryption, the choice of ROI directly affects the performance of the encryption algorithm, the smaller the number of ROI, the faster the encryption speed, and the lower the encryption effect. Consequently, we need a mathematical model to quantitatively analyze the parameters used to determine ROI. Game theory is that the two sides(or more sides) use the other party's strategy to change their confrontation strategies in an equal game to achieve the goal of winning. Behaviors with a competitive or antagonistic nature become game behaviors. Game theory is the study of mathematical models of strategic interaction between rational decision-makers. It has applications in all fields of social science, as well as in logic and computer science, such as it has been successfully applied to find state-of-the-art solutions to issues surrounding the next generation of wireless and communication networks [19]. Nash's bargaining solution was proposed by John Nash in his original paper [20]. Rosenkranz discussed the theory and application of the bargaining game in [21]. In 2006, Ahmad first attempt in using game theory for video compression, and the cooperative game leads to an optimal and fair bit allocation strategy based on the Nash bargaining solution [22]. We found that in the process of ROI encryption, based on different ROI parameter values, there is a competitive or antagonistic relationship between encryption performance and encryption speed, which is a game behavior. In this paper, We employ game theory to build a mathematical model to solve the conflict between encryption speed and encryption effect, and configure the conflict as a bargaining game.

Inspired by the above motivation, in this paper, we present a novel ROI optimization lossless medical image encryption and decryption algorithm based on game theory, optimize the ROI parameters, realize the accurate automatic selection of ROI, which can adapt to different types of image formats. Our contributions are summarized as follows:

- A new ROI selection method based on game theory is designed to achieve an accurate and automatic selection of ROI in medical images. It optimizes the ROI parameters according to the game results of encryption effect and encryption speed. Compared with other manually selected encryption schemes, it has obvious advantages.
- A lossless encryption and decryption algorithm for medical image ROI is proposed. The lossless decryption of medical images is crucial for medical staff and patients.
- The hiding of the position information of the ROI in the encryption process is realized, and the information

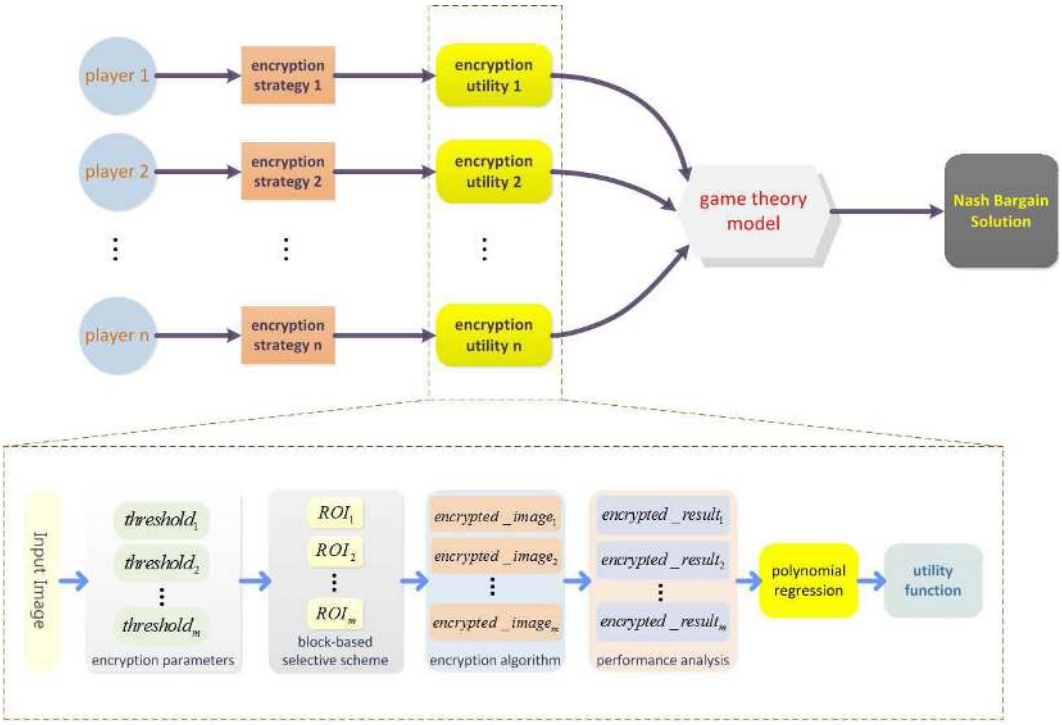

FIGURE 1. Optimization model of encryption parameters based on bargaining game and machine learning.

leakage caused by the embedding or transmission of the position information of the ROI is avoided.

The rest of this paper is organized as follows: Section 2 introduces the optimization model of encryption parameters based on the bargaining game and machine learning. Section 3 describes lossless image selective encryption/decryption scheme. Section 4 presents the experimental results and security analysis. Finally, Section 5 concludes the paper.

II. OPTIMIZATION MODEL OF ENCRYPTION PARAMETERS BASED ON BARGAINING GAME AND MACHINE LEARNING

In this section, the Nash bargaining solution is defined as a situation in which more players can mutually benefit from selecting an optimal parameter. The game model of encryption parameters optimization is as shown in Fig.1. The basic elements of game theory are players, strategies, and utility.

Players: N players compete for the use of a fixed resource in the game. Among them, the fixed resource refers to the profit of the encryption algorithm corresponding to the image segmentation scheme. N players correspond to N thresholds that can be selected in the image segmentation scheme. The winning player in the final game is the target threshold.

Strategies: The player's strategy is how to choose the threshold of the segmented image to ensure the safety and speed of the encryption algorithm.

The value range of each pixel in an 8-bit image is [0, 255], and the range of ROI thresholds for image segmentation is $[0, 255)$, with a total of 255 selectable thresholds. Therefore, the constraint of the N players' strategies is:

$$\sum_{i=1}^{N} t_i < 255 \times N \tag{1}$$

Utility: The utility function u_i of each player i reflects the encryption effect with the image segmentation threshold corresponding to the strategy selected by player i. For evaluating the encryption effect of an image, considering the security performance and encryption speed, the larger the threshold value, the better. Given a selected strategy threshold $t \in [0, 255)$, $t \in \mathbb{N}$, and strategy t executed by N players respectively, the utility set of the game is $u = (u_1(t), u_2(t), \ldots, u_N(t))$. Calculating the utility function of our optimization model includes two stages: constructing the encryption effect set function stage and fitting utility function stage:

1) CONSTRUCTING THE ENCRYPTION EFFECT SET FUNCTION STAGE

In the constructing encryption effect set function stage, we mainly analyze the encryption time and security performance of the encryption algorithm with different ROI thresholds. In this optimization model, encryption speed, peak signal-to-noise ratio(PSNR), structural similarity(SSIM), and information entropy are used as analysis indexes of encryption effect. Of course, according to actual application requirements, we can choose different performance analysis indicators, such as correlation coefficient, the number of pixels change rate(NPCR), and the unified averaged changed intensity(UACI).

For details on the algorithm used to encrypt images, see section 3.1. The specific construction steps of the encryption effect set function are as follows:

Step 1: When the image segmentation ROI thresholds are $t = 0, 1, 2, \ldots, 254$, the plain image is segmented and the region of interest is selected for encryption to obtain the cipher image set *SetEnImg*:

$$SetEnImg = \{EnImg(t(1)), EnImg(t(2)), \ldots, EnImg(t(255))\} \quad (2)$$

where $EnImg(t(i))$ denotes the cipher image when ROI threshold $t(i) = i - 1$.

Step 2: Sequentially record the encryption time required to obtain the cipher images when the ROI threshold $t = 0, 1, 2, \ldots, 254$, to obtain the encryption time set *SetEnTime*:

$$SetEnTime = \{EnTime(t(1)), EnTime(t(2)), \ldots, EnTime(t(255))\} \quad (3)$$

The distribution of encryption time set with the ROI threshold is shown in Fig.2.

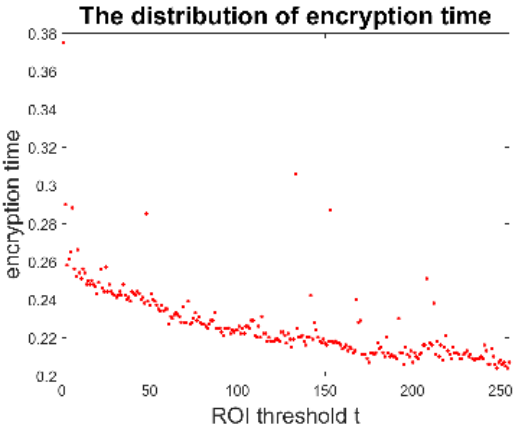

FIGURE 2. The distribution of encryption time with ROI threshold.

It can be seen that with the increase of the image segmentation ROI threshold, the encryption running time tends to become shorter gradually. This is because the larger the ROI threshold, the fewer image blocks that need to be encrypted, so the faster the calculation speed.

Step 3: According to the method of (4), calculate the PSNR between each element in the cipher image set SetEnImg and the plain image in turn, to obtain the set of peak signal-to-noise ratio *SetEnPSNR*:

$$\begin{cases} SetEnPSNR = \{EnPSNR(t(1)), EnPSNR(t(2)), \ldots, EnPSNR(t(255))\} \\ EnPSNR(t) = psnr(EnImg(t), Pimg) \\ psnr = 10\log_{10}\left(\frac{(2^L-1)^2}{MSE}\right) \\ MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(P1(i,j) - P2(i,j))^2 \end{cases} \quad (4)$$

PSNR is an index to measure image quality. Where $psnr()$ [23] is the peak signal to noise ratio function. *MSE* is the mean square error of the image $P1$ and the image $P2$. In our scheme, $P1$ denotes the elements of the cipher image set, and $P2$ is the plain image. H and W are the height and width of the image respectively. L is the number of bits per pixel, which is generally taken as 8. That is, the pixel gray level is 256. The distribution of peak signal-to-noise ratio with ROI threshold t is shown in Fig.3.

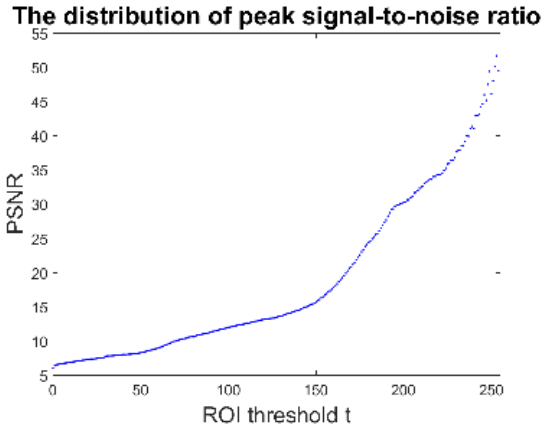

FIGURE 3. The distribution of peak signal-to-noise ratio with ROI threshold.

As can be seen from the distribution of Fig.3 that the larger the ROI threshold, the larger the PSNR, that is, the better the image reconstruction quality. The reason is that a larger ROI threshold corresponds to fewer encrypted areas, and the smaller the impact on image lossless restoration.

Step 4: According to the method shown in (5), the structural similarity between the elements of the cipher image set and the plain image is calculated in turn in order to obtain the structural similarity set *SetEnSSIM*:

$$\begin{cases} SetEnSSIM = \{EnSSIM(t(1)), EnSSIM(t(2)), \ldots, EnSSIM(t(255))\} \\ EnSSIM(t) = ssim(Enlmg(t), Pimg) \\ ssim(P1, P2) = l(P1, P2)c(P1, P2)s(P1, P2) \\ l(P1, P2) = \frac{2\mu_{P1}\mu_{P2} + C_1}{\mu_{P1}^2 + \mu_{P2}^2 + C_1} \\ c(P1, P2) = \frac{2\sigma_{P1}\sigma_{P2} + C_2}{\sigma_{P1}^2 + \sigma_{P2}^2 + C_2} \\ s(P1, P2) = \frac{\sigma_{P1P2} + C_3}{\sigma_{P1}\sigma_{P2} + C_3} \end{cases} \quad (5)$$

SSIM is an index to measure the similarity of two images. Where $ssim()$ [24] is the structural similarity function. μ_{P1}, μ_{P2} represent the average pixel values of images $P1$ and $P2$. $P1$ denotes the elements of the cipher image set, and $P2$ denotes the plain image. σ_{P1}, σ_{P2} are the variances of images $P1$ and $P2$. σ_{P1P2} represents the covariance of images $P1$ and $P2$. C_1, C_2, and C_3 are constants used to maintain stability. The range of SSIM is 0 to 1. When the

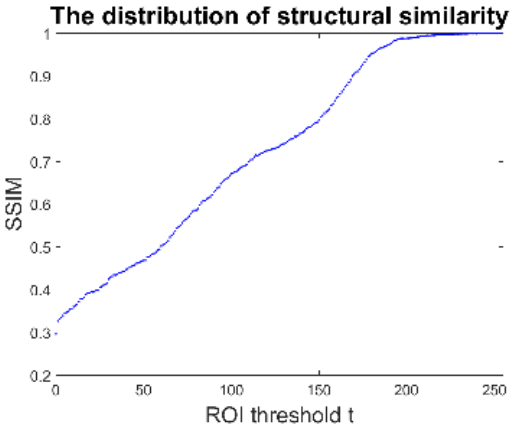

FIGURE 4. The distribution of structural similarity with ROI threshold.

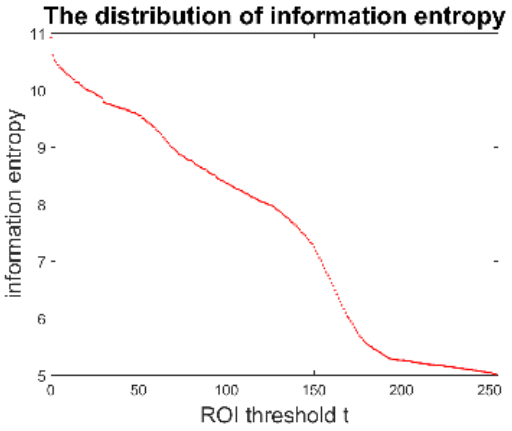

FIGURE 5. The distribution of information entropy with ROI threshold.

two images are the same, the value of SSIM is equal to 1. Fig.4 illustrates the distribution of the structural similarity set *SetEnSSIM* with the change of ROI threshold. Similar to the distribution of PSNR in Fig.3, the value of SSIM increases with the increase of the ROI threshold, that is, the quality of the image is better.

Step 5: The information entropy of each element of the cipher image set *SetEnImg* is calculated in turn. We obtain a cipher image information entropy set SetEnEntropy:

$$\begin{cases} SetEnEntropy = \{EnEntropy(t(1)), EnEntropy(t(2)), \\ \qquad\qquad \ldots, EnEntropy(t(255))\} \\ EnEntropy(t) = infoEntropy(Enlmg(t)) \\ infoEntropy(\phi) = -\sum_{i=0}^{2^L-1} p(\phi_i) \log_2 \dfrac{1}{p(\phi_i)} \end{cases} \tag{6}$$

Information entropy is one kind of important theoretical tool to measure the degree of image confusion. The more chaotic the encrypted image is, the greater the information entropy is. In (6), *infoEntropy* [15] denotes information entropy function. $p(\phi_i)$ represents the probability of a random event ϕ is ϕ_i. L is the pixel depth of the image. Fig.5 shows the calculation results of the information entropy of the 16-bit cipher image set.

The value of information entropy decreases monotonically as the ROI threshold increases in Fig.5. This means that the larger the ROI threshold, the fewer image blocks are selected for encryption. Correspondingly, the more uninteresting background areas ROB, the more unencrypted image blocks, the more uneven the final encrypted image pixels.

Step 6: According to the above encryption performance analysis results, we design the encryption effect set function *SetEnEffect*, as expressed by (7).

$$\begin{cases} SetEnEffect = \{EnEffect(t(1)), EnEffect(t(2)), \\ \qquad\qquad \ldots, EnEffect(t(255))\} \\ EnEffect(t) = 1/\log(\omega_1 K_1 EnTime(t) + \omega_2 EnPSNR(t) \\ +\omega_3 K_2 EnSSIM(t) + \omega_4 EnEntropy(t)) \end{cases} \tag{7}$$

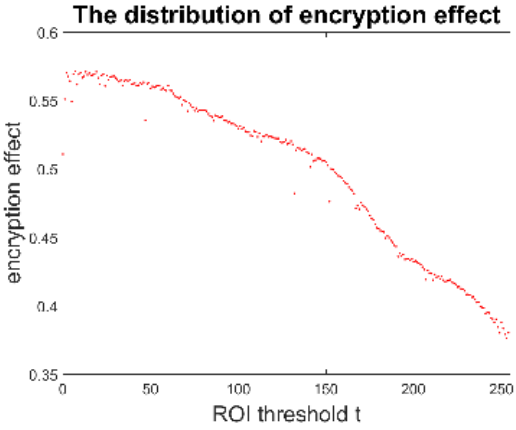

FIGURE 6. The distribution of encryption effect with ROI threshold.

where $\omega_1, \omega_2, \omega_3, \omega_4$ are the weights of the encryption performance set. ω_1 is the weight of the encryption time, ω_2 is the PSNR weight, ω_3 is the SSIM weight, ω_4 is the information entropy weight. K_1, K_2 are amplification factors, K_1 is encryption time amplification factor, K_2 is the amplification factor of SSIM. The encryption effect function is shown in Fig.6. It is easy to see that the larger the ROI threshold, the worse the encryption effect.

2) FITTING UTILITY FUNCTION STAGE

In the proposed game optimization scheme, we use the polynomial regression based on machine learning. It is a form of regression analysis in which the relationship between the independent variable x and the dependent variable y is modeled as an nth degree polynomial in x, to fit the utility function. The fitting method is described as follows:

Step 1: *SetEnEffect* obtained at the stage of constructing the encryption effect set function is scaled up to obtain *SetEnEffect*$'$, which will be used as the result set of polynomial linear regression.

$$SetEnEffect' = K \times SetEnEffect \tag{8}$$

where K is the scaling factor.

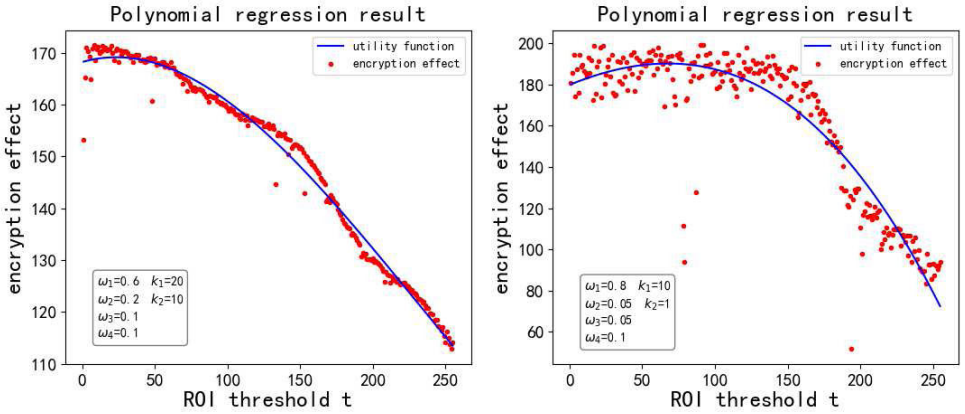

FIGURE 7. Fig.7(a) shows the polynomial regression result of encryption effect when $\omega_1 = 0.6, \omega_2 = 0.2, \omega_3 = \omega_4 = 0.1, K_1 = 20, K_2 = 10$. Fig.7(b) shows the result when $\omega_1 = 0.8, \omega_2 = 0.05, \omega_3 = 0.05, \omega_4 = 0.1, K_1 = 10, K_2 = 1$.

Step 2: Take $X = 1, 2, \ldots, 255$ as the input set.

Step 3: Increase the higher-order terms of X to get the high-order term input set $Poly\_X$

$$\begin{aligned} poly\_reg &= PolynomialFeatures(degree = 3) \\ Poly\_X &= poly\_reg.fit\_transform(X) \end{aligned} \tag{9}$$

where $PolynomialFeatures()$ represents the function of setting the number of terms of input X, and $poly\_reg.fit\_transform$ is the transformation of one-dimensional features into multi-dimensional features.

Step 4: The result set $SetEnEffect'$ is approximated by polynomial regression:

$$LinearRegression().fit(Poly\_X, SetEnEffect') \tag{10}$$

where $LinearRegression()$ represents a Linear Regression method.

Step 5: The coefficients of the polynomial are obtained according to the fitting result, and then the utility function u is generated.

The polynomial regression results of the encryption effect are shown in Fig.7. Fig.7(a) shows the polynomial regression result of encryption effect when $\omega_1 = 0.6, \omega_2 = 0.2, \omega_3 = \omega_4 = 0.1, K_1 = 20, K_2 = 10$. Fig.7(b) shows the result when $\omega_1 = 0.8, \omega_2 = 0.05, \omega_3 = 0.05, \omega_4 = 0.1, K_1 = 10, K_2 = 1$. It can be seen from the Fig.7(a)(b) that the utility function is a convex and compact set, so it can meet the requirements of the Nash bargaining game.

Initial Utility: When the player does not implement any strategy, the full image encryption scheme will be used as the initial strategy, that is, the image will not be divided, all image pixels will be encrypted, and then the encryption effect will be calculated according to the above method, and the utility function will be fitted to obtain the initial utility $d = (d_1, d_2, \ldots, d_N)$, we have $u > d, d_1 = d_2 = \ldots = d_N$.

In [19], Nash stated the four axioms for a fair bargain, specifying properties that the bargaining solution must satisfy. Therefore, to find the NBS(Nash Bargain Solution), we need to solve the following maximization problem:

$$\max \prod_{i=1}^{N} (u_i(t) - d_i) \quad \text{s.t.} \sum_{i=1}^{N} t_i \le 255 \times N \tag{11}$$

The above inequality constrained optimization problem can be solved by maximizing the following Lagrangean, using the theorem of Kuhn and Tucker [22].

III. LOSSLESS IMAGE SELECTIVE ENCRYPTION/ DECRYPTION SCHEME

In this section, we give the implementation details of the lossless image selective encryption and decryption scheme.

A. CHAOS KEY GENERATION

The image cryptosystem needs a large quantity of key streams, the chaotic system is a nonlinear dynamic system, and can produce the pseudo-random sequences of encryption security [25]–[27]. The sensitivity of the control parameters and the initial value by the chaotic systems can be used to ensure that the keyspace of the encryption system is large enough and the sensitivity enough of the key. In this lossless image selection encryption and decryption model, the Quantum Cell Neural Network hyperchaotic system is used to generate a security key [28]. The state equation of QCNN system is:

$$\begin{cases} \dot{x}_1 = -2a_1\sqrt{1-x_1^2}\sin x_4 \\ \dot{x}_2 = -2a_2\sqrt{1-x_2^2}\sin x_5 \\ \dot{x}_3 = -2a_3\sqrt{1-x_3^2}\sin x_6 \\ \dot{x}_4 = -a_4(x_1 - x_2 - x_3) + \dfrac{2a_1x_1\cos x_4}{\sqrt{1-x_1^2}} \\ \dot{x}_5 = -a_5(x_2 - x_1 - x_3) + \dfrac{2a_2x_2\cos x_5}{\sqrt{1-x_2^2}} \\ \dot{x}_6 = -a_6(x_3 - x_1 - x_2) + \dfrac{2a_3x_3\cos x_6}{\sqrt{1-x_3^2}} \end{cases} \tag{12}$$

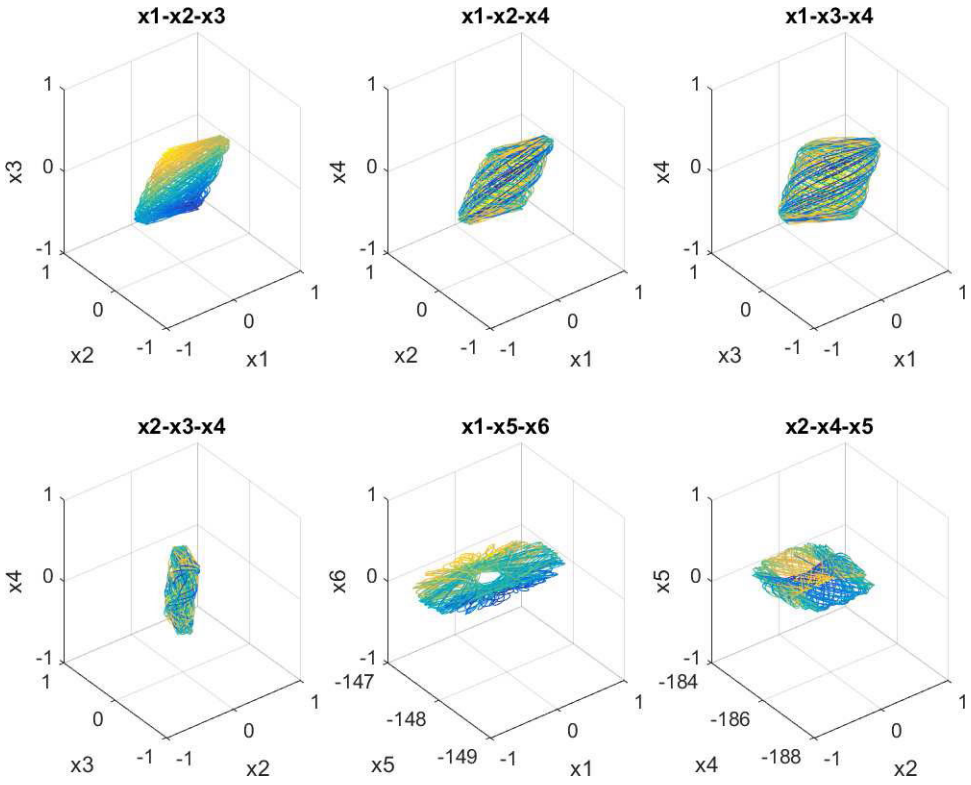

FIGURE 8. The attractor of the QCNN system.

where $x_1, x_2, x_3, x_4, x_5, x_6$ are the state variables, a_1, a_2, a_3, a_4, a_5, a_6 are the control parameters, Fig.8 shows the attractor of the QCNN system in three-dimensional space. We investigated the dynamic behavior of the QCNN system by calculating its Lyapunov exponents, as shown in Fig.9. When $a_1 = a_2 = a_3 = 0.28, a_4 > 0.907, a_5 = 0.2$, and $a_6 = 0.3$, the QCNN system is stable with four positive Lyapunov exponents. As a result, it is a hyperchaotic system. In addition, the simple connection of few quantum-dot cells (even two of them) can cause the onset of chaotic oscillation only with small differences of polarizations and template between cells, and it suggests the realization of nanoscale chaotic generators with high-frequency spectrum [29]. Based on the above reasons, QCNN can generate a large number of sufficiently sensitive random keys to ensure the security of encrypted images.

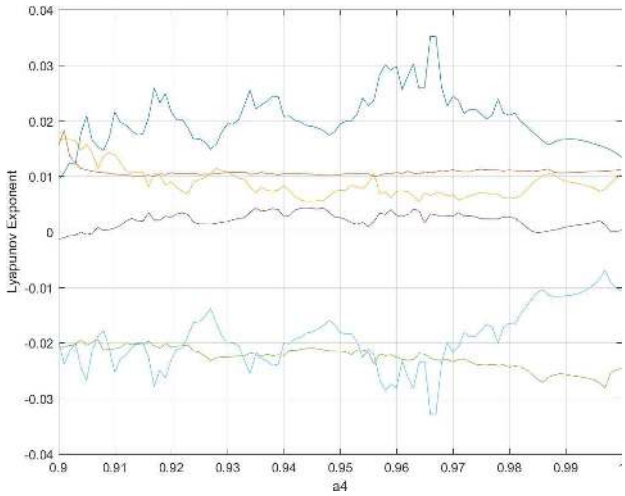

FIGURE 9. Lyapunov for the QCNN system.

B. ENCRYPTION ALGORITHM

To achieve lossless selective encryption of images, the algorithm contains five main phases: ROI block selection, conversion from spatial domain to transform domain, encryption of approximate coefficient vectors, lossless pixel-level format conversion, and encryption of the entire ROI. Firstly, through the parameter game optimization model proposed in Section 2, the image is segmented, and the ROI of the image is selected according to the optimal image segmentation threshold. Secondly, the two-dimensional lifting wavelet transform is used to transform the ROI region of the image from the spatial domain to the transform domain. Then, chaotic scrambling and diffusion operations are performed on the approximate coefficient vectors obtained by lifting wavelet transform. Next, to achieve the lossless decryption of the image, we perform pixel-level image format conversion on the image. Finally, the entire ROI area is completely encrypted, and the image is combined with the ROI area and the ROB area to obtain the final encrypted image. Moreover, the information entropy update key method is used to ensure

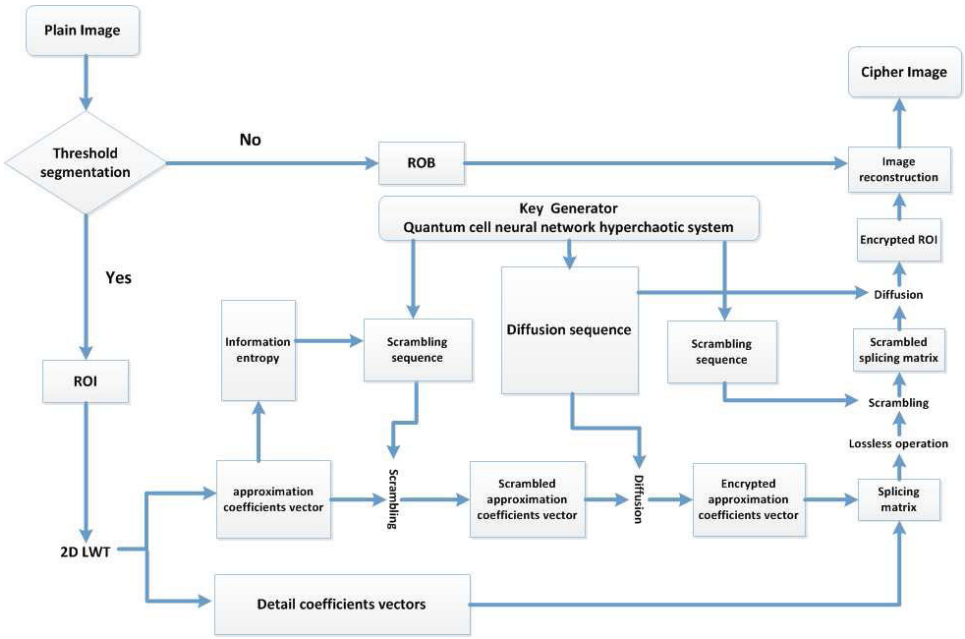

FIGURE 10. Encryption process.

that different plain images correspond to different encryption key streams, and a one-time security key operation is implemented to resist known plaintext attacks and selected plaintext attacks.

Fig.10 shows the encryption flow chart of the proposed algorithm. Assume the 8-bit gray medical image as a plain image, and the size is $M \times N$. Set the initial values $x_1, x_2, x_3, x_4, x_5, x_6$ and parameters $a_1, a_2, a_3, a_4, a_5, a_6$ of the quantum cell neural network hyperchaotic system(12) to be the user key. The detailed steps of encryption expatiate below:

1) ROI BLOCK SELECTION PHASE

Step 1.1 Given image block size is $n \times n$ (n is an integer divisible by M and N), segment the plain image into S blocks, $S = \lfloor \frac{M \times N}{n^2} \rfloor$. The image block size n can be optimized and selected by the method described in Section II.

Step 1.2 Calculate the average value of pixel grayscale of the image block according to (13)

$$e_i = mean(B_i) \tag{13}$$

where $mean()$ is the average function, B_i represents the $i-th$ image block, $i = 1, 2, 3, \ldots, S$.

Step 1.3 According to the game optimization method described in Section II, set the ROI threshold τ. The method of identifying the ROI from the image block is as follows:

If $e_i > \tau$, flag the image block B_i as the ROI.

Otherwise, flag the image block B_i as the ROB.

Step 1.4 All ROI blocks are stitched and rearranged to obtain an ROI matrix, denoted as M_{ROI}.

2) CONVERSION FROM SPATIAL DOMAIN TO TRANSFORM DOMAIN PHASE

At this phase, we use lifting wavelet transform to transform the ROI image matrix from the spatial domain to the transform domain. Extract the more critical low-frequency information in the ROI image block. Lifting wavelet transform is a new second-generation wavelet method for constructing wavelets using a lifting scheme in the time domain, which can be calculated more efficiently and needs less memory space compared with other traditional wavelets.

Perform two-dimensional lifting wavelet transform (2D LWT) on ROI matrix M_{ROI} to get the approximation coefficients vector CA_{ROI} and detail coefficients vectors CH_{ROI}, CV_{ROI}, and CD_{ROI}. Among them, the approximation coefficients vector is a low-frequency subband that characterizes more key information.

3) ENCRYPTION OF APPROXIMATE COEFFICIENT VECTORS PHASE

Step 3.1 Calculate the information entropy for the CA_{ROI}, denoted by h_{CA}.

$$h_{CA} = -\sum_{i=0}^{255} p(\phi_i) \log_2 \frac{1}{p(\phi_i)} \tag{14}$$

where $p(\phi_i)$ represents the probability of a random event ϕ is ϕ_i.

More importantly, the value of the information entropy is very sensitive to the image information [30]. Since CA_{ROI} is the low-frequency information of the plain image ROI, h_{CA} is related to plaintext, and different plain images have completely different information entropy. Therefore, $CA_{ROI}{}'s$

information entropy is used to update user keys to influence the generation and selection of key streams.

$$[key'] = [key] + \frac{\mathrm{hc}_A}{\mathrm{h}_{CA} + 1} \bmod 1 \tag{15}$$

where key is the user keys and key' represents the user keys related to the plaintext after the update. In the proposed algorithm, key refers to the initial value and parameters of the QCNN hyperchaotic system.

Step 3.2 Using the updated $[key']$ as the initial value and control parameters, iterate (12) to generate the hyperchaotic matrix M_{QCNN}. According to the order from left to right, from top to bottom, the matrix elements are taken to form the hyperchaotic sequence S_{CA}, which is used for scrambling CA_{ROI}.

$$\begin{aligned} [S_{CA}\_sorted, P] &= sort\,(S_{CA}) \\ CA_{ROI^p} &= CA_{ROI}(P) \end{aligned} \tag{16}$$

where S_{CA}_sorted is an ascending sequence after sorting the elements of S_{CA}, P represents the position information of the elements of S_{CA}_sorted in S_{CA} after sorting. CA_{ROI^p} is the scrambled ROI low-frequency subband information. The scrambling operation can disturb the position information of the elements in the CA_{ROI} and destroy the correlation of adjacent elements.

Step 3.3 Continue to take elements from the matrix in order from top to bottom and left to right to form the hyperchaotic sequence D_{CA}. Perform a diffusion operation on $CA_{ROI^{pd}}$:

$$\begin{aligned} CA_{ROI^{pd}}(i+1) = &\left(\left\lfloor D_{CA} \times 10^4 \right\rfloor \bmod H\right)(i+1) \\ &\oplus CA_{ROI^p}(i+1) \oplus CA_{ROI^{pd}}(i) \end{aligned} \tag{17}$$

where $i = 1, 2, 3, \ldots, length(CA_{ROI}) - 1$, $H = 256$.

Step 3.4 The encrypted $CA_{ROI^{pd}}$ and detail coefficients vectors of the ROI matrix $M_{ROI}(CH_{ROI}, CV_{ROI}, CD_{ROI})$ are spliced according to the original M_{ROI} size. Obtain a preliminary encrypted ROI and record it as ROI^{en}:

$$ROI^{en} = [CA_{ROI^{pd}}, CD_{ROI}; CV_{ROI}, CH_{ROI}] \tag{18}$$

4) LOSSLESS PIXEL-LEVEL FORMAT CONVERSION PHASE

Step 4.1 Because after the 2D LWT, the pixel values of the detail coefficients vectors do not meet the normal image standard, ROI^{en} need to be normalized at first:

$$ROI^{en}\_Nor = mapminmax(ROI^{en}, 0, 1) \tag{19}$$

where $mapminmax()$ processes matrix by normalizing the minimum and maximum values of each row to [0, 1].

Step 4.2 Map the ROI^{en}_Nor to 16-bit pixels:

$$ROI^{en}\_Nor16 = im2uint16(ROI^{en}\_Nor) \tag{20}$$

where the function $im2uint16()$ converts the intensity image to 16-bit unsigned integers.

In medical image encryption, lossless decryption is crucial, and even affects the doctor's diagnosis. In the algorithms proposed in [31]–[33], they all encrypt plain images in the frequency domain, but lossless decryption cannot be achieved through their frequency domain encryption algorithms. In our scheme, the ROI pixel format is changed to a 16-bit image, which avoids the loss of image information during the decryption process. Therefore, our encryption algorithm can better protect the integrity of image information, and is more suitable for medical image encryption or other encryption fields that require high image integrity. At the same time, the image information is further hidden due to changes in the image format [8].

5) ENCRYPTION OF THE ENTIRE ROI PHASE

Step 5.1 Using the same method as intercepting S_{CA} and D_{CA}, select hyperchaotic sequences S_{ROI} and D_{ROI} from different starting positions, which are used for scrambling and diffusion of the entire ROI area, respectively.

Step 5.2 Scrambling the lossless format conversion results:

$$\begin{aligned} [S_{ROI}\_sorted, P] &= sort\,(S_{ROI}) \\ ROI^{en}\_Nor16^p &= ROI^{en}\_Nor16(P) \end{aligned} \tag{21}$$

Similar to step 3.2, S_{ROI}_sorted is an ascending sequence after sorting the elements of S_{ROI}. $ROI^{en}\_Nor16^p$ denotes the scrambled result of ROI^{en}_Nor16.

Step 5.3 Diffusion of lossless format conversion results:

$$\begin{aligned} ROI^{en}\_Nor16^{pd}(i+1) = &\left(\left\lfloor D_{ROI} \times 10^9 \right\rfloor \bmod H\right)(i+1) \\ &\oplus ROI^{en}\_Nor16^p(i+1) \\ &\oplus ROI^{en}\_Nor16^{pd}(i) \end{aligned} \tag{22}$$

where $i = 1, 2, 3, \ldots, length(ROI^{en}\_Nor16) - 1$, $H = 65536$.

Step 5.4 Put the encrypted $ROI^{en}\_Nor16^{pd}$ and ROB back to the original position of the plain image to get the final cipher image.

For the hyperchaotic sequences $S_{CA}, D_{CA}, S_{ROI}, D_{ROI}$ used in the encryption operation in the above algorithm, the starting position value selected from the matrix can be freely set by the user to further improve the security of the encryption system.

C. DECRYPTION ALGORITHM

The proposed encryption/decryption scheme is symmetric. The decryption process is the inverse of the encryption process. The decryption flowchart is shown in Fig.11. Since the value range of cipher ROI is [0, 65535], the value range of ROB is [0, 255], we can still use the block-based selection scheme proposed in Section 3.2 to distinguish between encrypted ROI and ROB, instead of sending the location information of ROI to the receiver or embedding the location information of ROI into the image as most algorithms in other literatures. In this way, the possibility of leakage of encrypted location information during transmission and storage can be reduced.

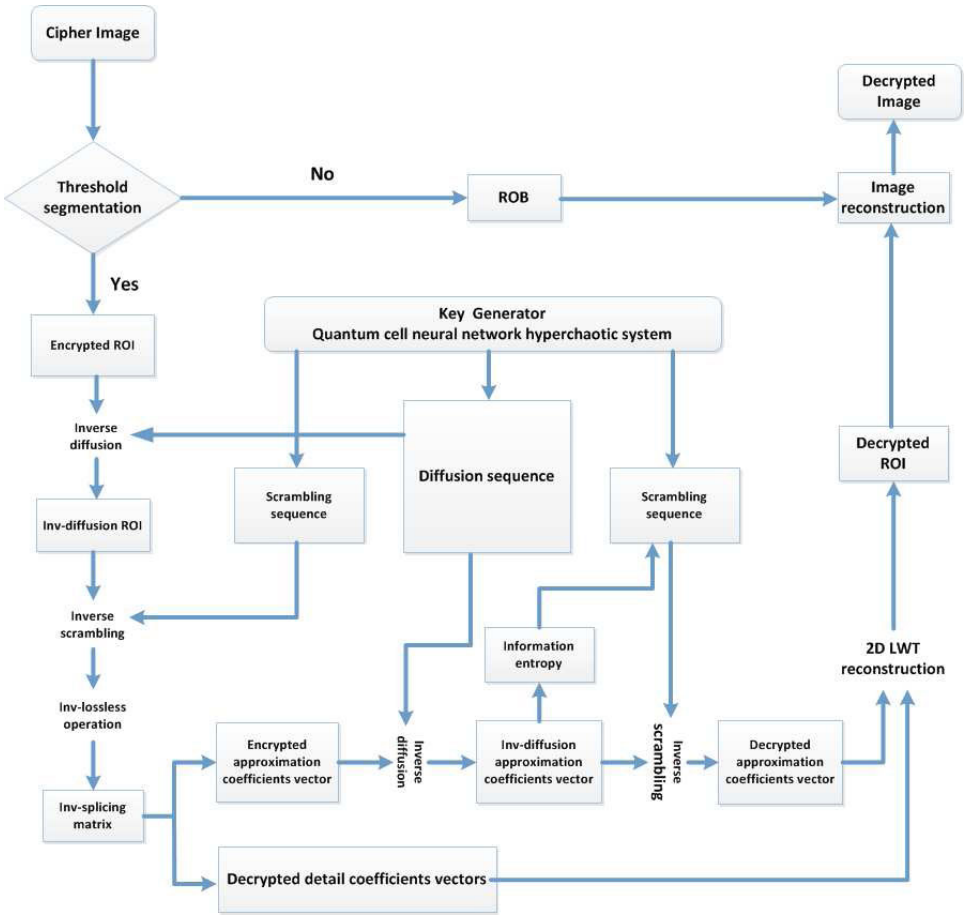

FIGURE 11. Decryption process.

IV. EXPERIMENTS AND ANALYSIS

A. RESULTS

In this section, the experiments have been performed on MATLAB R2015b. Various experiments have been conducted to verify the performance of our proposed encryption scheme. We consider medical images of different structures and types as the plain images. To illustrate the effect of encryption experiments, the following compares our ROI selective algorithm and the corresponding full encryption algorithm for encryption analysis, respectively. Although we do experimental analysis in grayscale medical images, our algorithm can also be applied to color medical images, that is, the three color components R, G, and B can be encrypted using the proposed encryption algorithm.

Fig.12 shows the full encryption results of four types of grayscale medical images, Fig.12(a), Fig.12(e), Fig.12(i), Fig.12(m) represent Thorax 7.0 MIP, Thorax 5.0 B31f, CT_SLICES, and MRI image Brain plain images, respectively. Fig.12(b), Fig.12(f), Fig.12(j), Fig.12(n) are the approximate coefficient vectors of two-dimensional lifting wavelet transform in the plain images. Fig.12(c), Fig.12(g), Fig.12(k), and Fig.12(o) are the intermediate results of approximate coefficient vector encryption. Fig12(d), Fig.12(h), Fig.12(l), Fig.12(p) mean the final encrypted images after full encryption of the plain images Fig.12(a), Fig.12(e), Fig.12(i), Fig.12(m).

To compare and analyze our ROI encryption algorithm, the results of encryption and decryption of the proposed algorithm of four identical plain images are given in Fig.13. We choose that the image segmentation size is 8×8, and the optimal segmentation threshold τ is 23, which is determined by the encryption parameter optimization model based on the bargaining game. See Section II for details.

Because the pixel value of ROB is $[0, 255]$ and the pixel value of ROI is $[0, 65535]$, which has been described in Section 3.2, the whole image type is changed from an 8-bit pixels to 16-bit pixels. As a result, the ROB is visually dark, it is difficult to visually visualize the ROB. The encryption results Fig.13(b), Fig.13(e), Fig.13(h), Fig.13(k) show that our scheme protects the image information well, and the image content cannot be distinguished from the subjective visual effects. Moreover, the decryption results Fig.13(c), Fig.13(f), Fig.13(i), Fig.13(l) restore the original images.

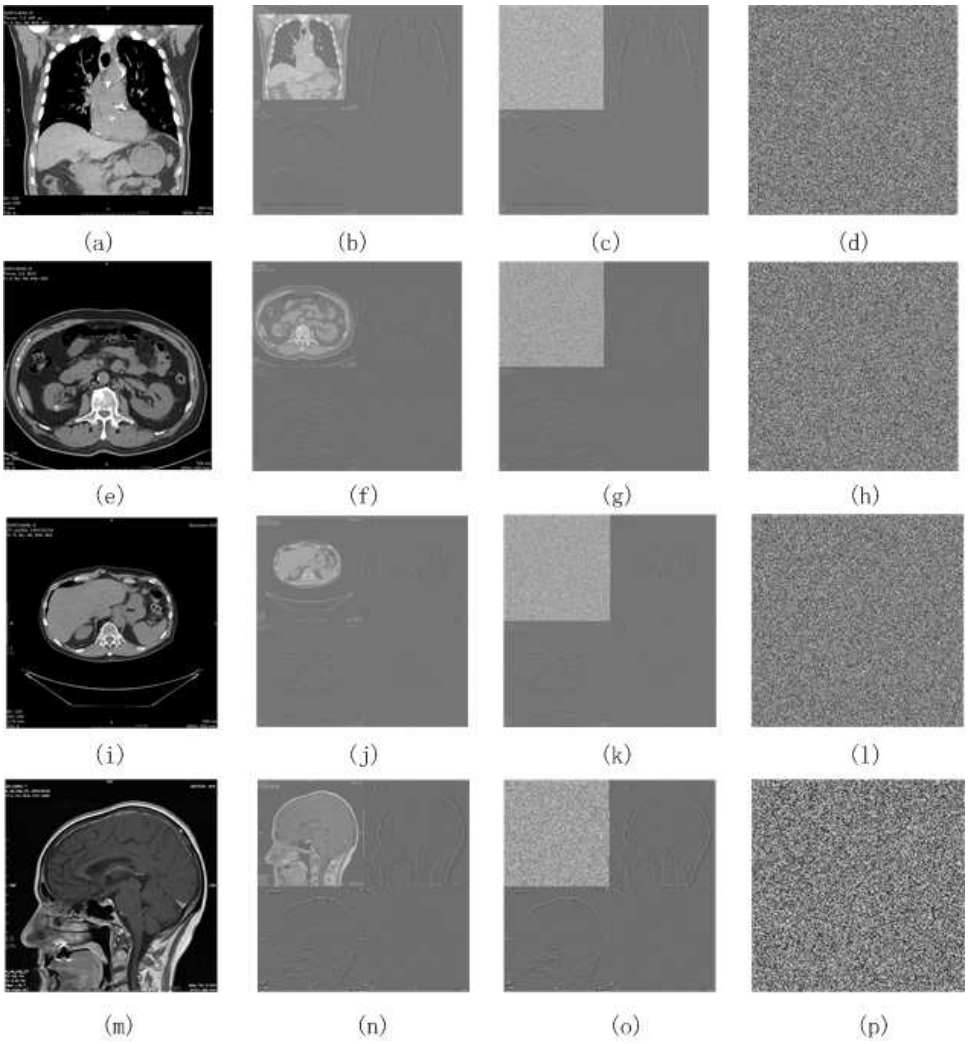

FIGURE 12. Gray medical images with full encryption. (a), (e), (i), (m) show Thorax 7.0 MIP, Thorax 5.0 B31f, CT_SLICES,and MRI image Brain plain images. (b), (f), (j), (n) show the results of the 2D-LWT in the plain images. (c), (g), (k), (o) show intermediate results of the encrypted the approximate coefficient vectors. (d), (h), (l), (p) show the final cipher images after full encrypting.

TABLE 1. ROI analysis.

Plain Images	τ	The number of the ROI	The size of the encrypted image	ROI ratio	PSNR
Thorax 7.0 MIP	0	166784	262144	0.636	5.989
	23	148096	262144	0.565	7.358
	70	115456	262144	0.440	9.976
	150	59264	262144	0.226	15.660
Thorax 5.0 B31f	0	168960	262144	0.644	4.414
	23	154432	262144	0.589	5.091
	70	74560	262144	0.284	10.267
	150	7808	262144	0.030	25.288
CT_SLICES	0	95744	262144	0.365	6.989
	23	78912	262144	0.301	8.565
	70	46912	262144	0.179	12.926
	150	3968	262144	0.015	26.542
MRI image Brain	0	102400	102400	1.000	1.879
	23	68992	102400	0.674	4.672
	70	39168	102400	0.382	8.030
	150	2880	102400	0.028	23.947

B. ROI ANALYSIS

The proposed scheme provides a novel way to select the ROI, which allows users to choose the encryption parameters according to the optimal method based on game theory. In different application scenarios, users will have different application requirements for the encryption system, sometimes

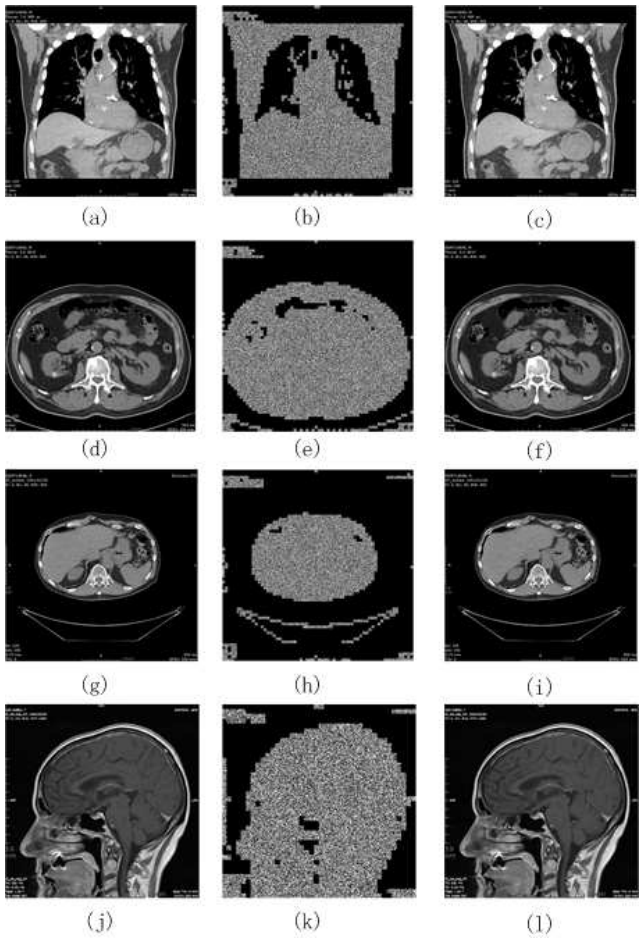

FIGURE 13. The encryption/decryption results of the proposed algorithm. (a), (d), (g), (j) show four different types and structure plain images. (a)Thorax 7.0 MIP, (d)Thorax 5.0 B31f, (g)CT_SLICES,and (j)MRI image Brain. (b), (e), (h), (k)are the cipher images. (c), (f), (i), (l) are the decrypted images.(τ is 23, image segmentation size is 8 × 8)

requiring higher encryption efficiency and sometimes requiring better security. When users have different needs for encryption performance, they can choose different encryption weight values in (7), and the proposed game model will get the optimal threshold. When the encryption weight values $\omega_1 = 0.6, \omega_2 = 0.2, \omega_3 = \omega_4 = 0.1, K_1 = 20, K_2 = 10$ in (7), the Nash equilibrium solution of this bargaining game is 23, that is, the optimal ROI threshold is 23.

We evaluate the influence of the ROI threshold on the encryption effect based on the number of the ROI and the PSNR between the plain images and the cipher images. The number of ROI indicates the number of areas that need to be encrypted. The more ROI number, the more areas that need to be encrypted, and the longer the encryption takes. PSNR is an objective criterion used to evaluate the fidelity of an image between plain image and cipher image. Generally speaking, when PSNR is lower than 15, the cipher image and the plaint image cannot be visually correlated, if PSNR is greater than 15, the image protection is poor. Table 1 presents the ROI data results of plain images for different ROI thresholds (i.e. $\tau = 0, 23, 70$, and 150 respectively). Among them, the ROI ratio represents the percentage of ROI in the plain image. It can be seen from Table 1 that for all encryption results, as the threshold τ increases, the number of ROI has a clear downward trend, while PSNR has a clear upward trend. The proposed game optimization parameter selection method not only protects the image security, but also reduces the calculation amount of ROI encryption. In our algorithm model, we have achieved a balance between encryption security performance and encryption speed.

C. ENCRYPTION KEY SPACE ANALYSIS

An excellent encryption algorithm should have enough keyspace to defend against brute force attacks. In the proposed algorithm, the security keys are composed of the initial values $x_1, x_2, x_3, x_4, x_5, x_6$ and control parameters $a_1, a_2, a_3, a_4, a_5, a_6$ of the quantum cell neural network hyperchaotic system(12), each precision of key is 10^{-16}, namely, the size of keyspace is 10^{192}. As a result, this keyspace is big enough for brute-force attacks [34].

D. STATISTICAL ANALYSIS

It is crucial to resist statistical analysis in case of leaking the image characteristics.

1) HISTOGRAM ANALYSIS

Histogram analysis is an important metric used in the evaluation of the robustness of an image encryption scheme [35]. An image histogram shows the distribution of the pixel values within an image. In our proposed scheme, only the ROI of the plain image is encrypted, and thus we examine only the histogram of the ROI. Fig.14 illustrates the ROI histograms of the plain images, cipher images, and decrypted images of the ''Thorax 7.0 MIP'', ''Thorax 5.0 B31f'', and ''CT_SLICES'', respectively, when the threshold $\tau = 23$. The experimental results prove that the pixel values in the encrypted image are evenly distributed, similar to white noise. This shows that we have successfully changed the distribution relationship of pixel values, and our algorithm can effectively resist statistical attack.

For quantity analyses of the image histogram, we use variances of histograms to evaluate the uniformity of cipher images. The lower value of variances indicates the higher uniformity of cipher images. In addition, we also analyze the two variances of the encrypted images with different secret keys on the same plain image. When the secret keys are different, the closer of the two values of variances represents the higher uniformity of cipher images. The variance of histograms is calculated by [36]:

$$\mathrm{var}(Z) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} \left(z_i - z_j\right)^2 \tag{23}$$

where Z denotes the vector of the histogram values, z_i and z_j are the numbers of pixels, which gray values are equal to i and j respectively. Since our encrypted image is a 16-bit image,

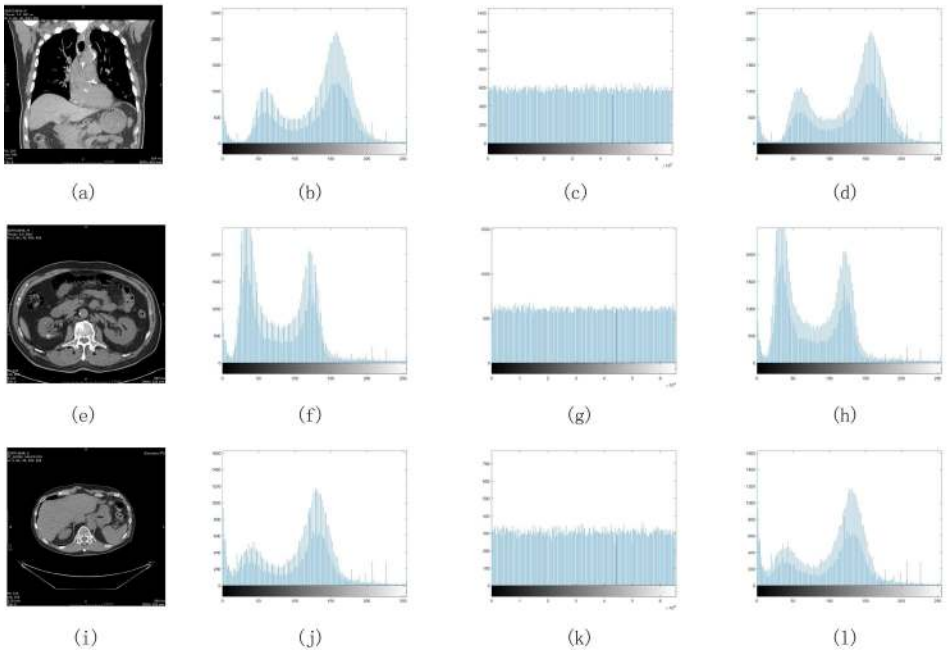

FIGURE 14. (a),(e),(i) are plain images (b),(f),(j) are histogram of plain image (c),(g),(k) are histogram of cipher images (d),(h),(l) are histogram of decrypted images.

$Z = \{z_1, z_2, \ldots, z_{65536}\}$. In this experiment, we only change the initial values x_1, x_2, x_3, x_4, x_5, x_6 in the secret keys to calculate two variances of histograms of two cipher images by (23) from the same plain image with different secret keys. we set four different secret keys:

$$\begin{cases} key0 = \{-0.131, -0.135, -0.123, -184.9, 147.3414, \\ \quad -196.852, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\} \\ key1 = \{-0.161, -0.155, -0.223, -184.8, 147.6414, \\ \quad -196.652, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\} \\ key2 = \{-0.121, -0.145, -0.201, -184.6, 147.5321, \\ \quad -196.923, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\} \\ key3 = \{-0.231, -0.175, -0.245, -185.0, 147.4414, \\ \quad -197.052, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\} \\ key4 = \{-0.331, -0.235, -0.258, -185.1, 147.6414, \\ \quad -196.752, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\} \end{cases} \tag{24}$$

We calculate the variances of histograms of encrypted "Throax 7.0 MIP", "Throax 5.0 B31f" and "CT_SLICES". The results are listed in Table 2. To measure the stability of the histogram variance of different images encrypted with different secret keys, the variance stability rate is defined as [36]:

$$\eta_{var}\left(z_0, z_\zeta\right) = \frac{\left|\text{var}\left(Z_\zeta\right) - \text{var}\left(Z_0\right)\right|}{\text{var}\left(Z_0\right)} \times 100\% \tag{25}$$

where Z_0 is the cipher image obtains by encrypting the plain image using $key0$. And ζ represents the $key1$,$key2$,$key3$, and $key4$. Z_ζ is the encrypted results using ζ. The numerical analysis of histogram variance is listed in Table 3. The average variance of the algorithm [36] is 3.88%. In this algorithm, The variance fluctuation range caused by different keys is less than 1.07%, which shows that our algorithm has excellent histogram uniformity and stability. The simulation results indicate that our algorithm can effectively resist statistical analysis attacks.

TABLE 2. Variances of histograms compared among different secret keys in the proposed algorithm.

Cipher image	$key0$	$key1$	$key2$	$key3$	$key4$
Thorax 7.0 MIP	4.0184	4.0215	3.9950	3.9858	4.0031
Thorax 5.0 B31f	4.0128	3.9848	3.9929	4.0072	3.9699
CT_SLICES	3.9899	3.9815	3.9810	3.9860	3.9531
Average	4.0070	3.9959	3.9896	3.9930	3.9753

TABLE 3. Percentage of variances difference of histograms compared with different secret keys.

Cipher image	$key1(\%)$	$key2(\%)$	$key3(\%)$	$key4(\%)$
Thorax 7.0 MIP	0.08	0.58	0.81	0.38
Thorax 5.0 B31f	0.70	0.50	0.14	1.07
CT_SLICES	0.21	0.22	0.10	0.92
Average	0.33	0.43	0.35	0.79

2) INFORMATION ENTROPY

Information entropy is an important tool to measure the degree of image confusion. The encryption process is a process of increasing information entropy. The larger the information entropy, the more chaotic the image information. The calculation method of information entropy is (6). After calculation, the ideal information entropy of 8-bit encrypted images is 8. Similarly, if the cipher image pixels

are represented by 16 bits, then the value of the information entropy should be $I(\phi) = \sum_{i=0}^{65535} p(\phi_i) \log_2 \frac{1}{p(\phi_i)}$. So in an ideal state, the absolute random cipher image information entropy is 16. Since we performed the lossless format conversion phase, the image format changed from 8 bits to 16 bits. Therefore, the information entropy of the image encrypted by our algorithm is close to 16, not to 8. To compare the encryption effect, we also calculated the 8-bit information entropy of the encrypted image without changing the image format and without the lossless transformation stage.

When the ROI threshold is 23, the calculation results of information entropy are listed in Table 4. Obviously, the value of the information entropy of 8-bit encrypted images and 16-bit encrypted images are infinitely close to the ideal values.

TABLE 4. Information entropy for the cipher images.

Image	Plain image	Cipher image (16 bit)	Cipher image (8bit)
Thorax 7.0 MIP	7.1398	15.6367	7.9994
Thorax 5.0 B31f	7.0689	15.6574	7.9994
CT_SLICES	7.0611	15.3083	7.9992
MRI image Brain	7.1160	15.2133	7.9986
Ref. [39]	7.7748	–	7.9989
Ref. [17]	7.6633	–	7.9916

In addition, the local entropy can better represent the randomness of the image, it may be defined as [37]:

$$\bar{H}_{k,T_B}(m) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{26}$$

where non-overlapping image blocks $S_1, S_2, \ldots, S_k$ with T_B pixels for a test image S are randomly chosen, $H(S_i)$ represents information entropy for image block S_i, and k is the block number. We calculate the local entropies for different images with $k = 30$ and $T_B = 1936$, and list the results in Table 5. Under this condition, the ideal local entropy of 8-bit encrypted images is 7.902469317 [38]. For the convenience of experiment comparison, we also generate the two different types of cipher images mentioned above, namely 8-bit cipher image and 16-bit cipher image. From Table 5, all the 8-bit cipher images' local entropies are more than 7.901, and close to the ideal value. This better proves our algorithm has good local randomness and can effectively resist entropy attacks.

TABLE 5. Local entropy for the cipher images.

Image	Cipher image (16 bit)	Cipher image (8bit)
Thorax 7.0 MIP	10.8887	7.9017
Thorax 5.0 B31f	10.8896	7.9022
CT_SLICES	10.8894	7.9052
MRI image Brain	10.8891	7.9020
Ref. [38]	–	7.9018
Ref. [40]	–	7.9029

3) CORRELATION ANALYSIS

The correlation of adjacent pixels reflects the degree of correlation of pixel values at adjacent positions of the image. A good image encryption algorithm should reduce the adjacent correlation and try to achieve the zero correlation. Generally, the horizontal, vertical, and diagonal pixels of the image must be analyzed. The correlation test is applied by taking randomly N random pairs of adjacent pixels from the plain image or the cipher image. The correlation coefficient r_{xy} is calculated using the following equation [38]:

$$\begin{aligned} r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \\ E_x &= \frac{1}{N} \times \sum_{i=1}^{N} x_i \\ D_x &= \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))^2 \\ cov(x,y) &= \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \end{aligned} \tag{27}$$

We randomly selected 4000 pairs of adjacent pixels along the horizontal, vertical, and diagonal directions in the plain images and cipher images of "Thorax 7.0 MIP" and "Thorax 5.0 B31f" for correlation analysis. The test results are shown in Fig.15 $(a) - (f)$ and Fig.16 $(a) - (f)$, respectively.

TABLE 6. The correlation coefficients of cipher images.

Image	Horizontal	Vertical	Diagonal
Thorax 7.0 MIP	-0.0090	-0.0069	-0.0034
Thorax 5.0 B31f	0.0072	0.0260	0.0024
CT_SLICES	0.0043	-0.0039	-0.0037
MRI image Brain	0.0010	0.0015	0.0081
Ref. [12]	0.0193	-0.0154	0.0032
Ref. [41]	-0.0019	0.0105	-0.0019

As can be seen from Table 6, the correlation coefficients of cipher images are approximately equal to 0. This means that adjacent pixels in the cipher images have extremely low correlation in the horizontal, vertical, and diagonal directions. As a result, the proposed encryption scheme is sufficient to resist statistical attacks based on pixel correlation.

E. DIFFERENTIAL ATTACK ANALYSIS/PLAINTEXT SENSITIVITY ANALYSIS

The number of pixel changing rate(NPCR) and the unified averaged changed intensity(UACI) are commonly used in checking the avalanche effect and plaintext sensitivity, which are defined as [40]:

$$\text{NPCR} = \frac{\Sigma_{ij} D(i,j)}{m \times n} \times 100\% \tag{28}$$

where M is the total number of pixels in the $D(i,j)$, $D(i,j)$ is defined as [40]:

$$\text{D(i, j)} = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$\text{UACI} = \frac{1}{m \times n} \left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{65535} \right] \times 100\% \tag{29}$$

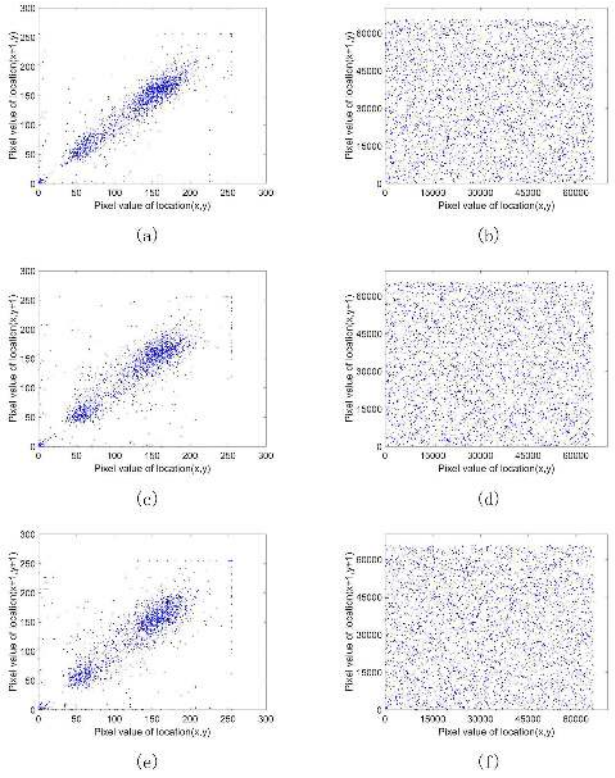

FIGURE 15. "Thorax 7.0 MIP" image correlation of two adjacent pixels.

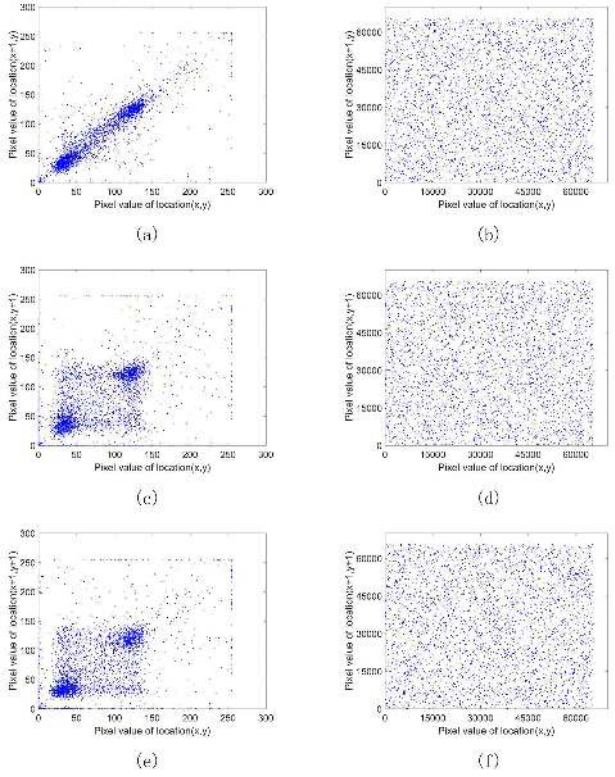

FIGURE 16. "Thorax 5.0 B31f" image correlation of two adjacent pixels.

where C_1 and C_2 denote the two cipher-images that have a one-bit change in the same plain image. For a 16-bit grayscale image, the ideal value for UACI is approximately 33.3333%, while the ideal value for NPCR is approximately 99.9985%. We tested different images to obtain NPCR and UACI using the proposed encryption scheme. The test results are listed in Table 7, which shows that our encryption scheme meets the robustness requirements against differential attacks. Moreover, this result also proves that our algorithm is highly sensitive in plaintext.

TABLE 7. The UACI and NPCR of two cipher-images.

	Thorax 7.0 MIP	Thorax 5.0 B31f	CT_SLICES	MRI image Brain
UACI	33.2836%	33.3025%	33.3136%	33.4272%
NPCR	99.9984%	99.9992%	99.9989%	99.9980%

F. KEY SENSITIVITY ANALYSIS

A good encryption scheme must be sensitive enough to slight changes in the key, both encryption and decryption processes should be sensitive to key [42]. When the key is slightly different, two completely different cipher images will be generated. In other words, even if the approximate range of the key guessed by the attacker, as long as it is slightly different from the correct key, it will get completely different decryption results.

Given $KEY = \{x_1, x_2, x_3, x_4, x_5, x_6, a_1, a_2, a_3, a_4, a_5, a_6\} = \{-0.131, -0.135, -0.123, -184.9, 147.3414, -196.852, 0.28, 0.29, 0.285, 0.5, 0.2, 0.3\}$. We choose six of these parameters to make slight changes to test the key sensitivity, and obtain the mismatch key $EKEY1$,$EKEY2$, $EKEY3$, $EKEY4$, $EKEY5$, $EKEY6$:

$$\begin{cases} EKEY1 = \{x_1 + 10^{-16}, x_2, x_3, x_4, x_5, \\ \qquad x_6, a_1, a_2, a_3, a_4, a_5, a_6\} \\ EKEY2 = \{x_1, x_2 + 10^{-16}, x_3, x_4, x_5, \\ \qquad x_6, a_1, a_2, a_3, a_4, a_5, a_6\} \\ EKEY3 = \{x_1, x_2, x_3 + 10^{-16}, x_4, x_5, \\ \qquad x_6, a_1, a_2, a_3, a_4, a_5, a_6\} \\ EKEY4 = \{x_1, x_2, x_3, x_4, x_5, x_6, \\ \qquad a_1, a_2, a_3, a_4 + 10^{-16}, a_5, a_6\} \\ EKEY5 = \{x_1, x_2, x_3, x_4, x_5, x_6, \\ \qquad a_1, a_2, a_3, a_4, a_5 + 10^{-16}, a_6\} \\ EKEY6 = \{x_1, x_2, x_3, x_4, x_5, x_6, \\ \qquad a_1, a_2, a_3, a_4, a_5, a_6 + 10^{-16}\} \end{cases} \tag{30}$$

In encryption processes, we use the mismatch key to encrypt the same plain image "Thorax 7.0 MIP" to get six different cipher images, as shown in Fig.17, and we calculated the NPCR and UACI values between the encrypted images using the KEY and the mismatch key based on the same plain image. and the calculation results are listed in Table 8.

In decryption processes, if the decryption key and the encryption key have a minimal error, then the decryption key cannot be used to restore the cipher image correctly, as shown in Fig.18. Similarly, we calculated the NPCR and UACI values between the decrypted image using the KEY

TABLE 8. The NPCR and UACI values between the encrypted images using the KEY and the mismatch key based on the same plain image "Thorax 7.0 MIP".

	$EKEY1$	$EKEY2$	$EKEY3$	$EKEY4$	$EKEY5$	$EKEY6$
UACI	99.9588%	99.9332%	99.9602%	99.6293%	99.9608%	99.6266%
NPCR	33.2743%	33.2494%	33.1900%	33.1317%	33.1519%	33.1305%

TABLE 9. The NPCR and UACI values between the decrypt the image using the KEY and the mismatch key based on the same cipher image "Encrypted Thorax 7.0 MIP".

	$EKEY1$	$EKEY2$	$EKEY3$	$EKEY4$	$EKEY5$	$EKEY6$
UACI	98.2018%	98.2140%	98.2667%	98.2349%	98.2032%	98.2478%
NPCR	36.3987%	36.4163%	36.4084%	36.3011%	36.4732%	36.3071%

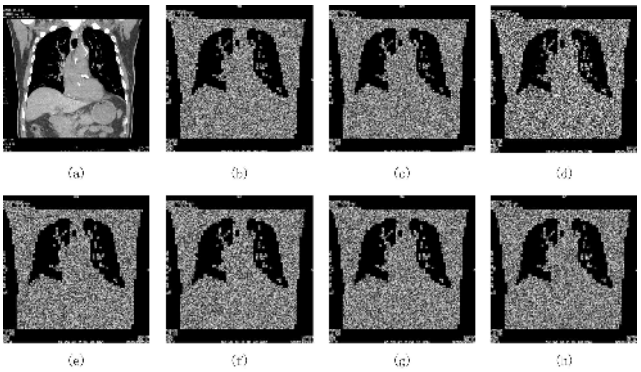

FIGURE 17. Key sensitivity test for Thorax 7.0 MIP in encryption processes (a) Plain image Thorax 7.0 MIP (b) Encrypted image with *EKEY* (c) Encrypted image with *EKEY*1 (d) Encrypted image with *EKEY*2 (e) Encrypted image with *EKEY*3 (f) Encrypted image with *EKEY*4 (g) Encrypted image with *EKEY*5 (h) Encrypted image with *EKEY*6.

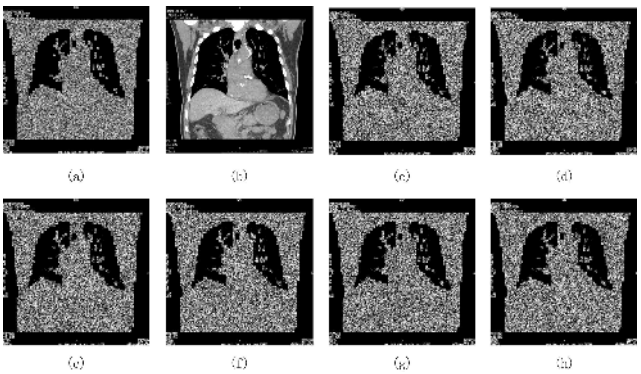

FIGURE 18. Key sensitivity test for the encrypted Thorax 7.0 MIP in decryption processes (a) Cipher image encrypted Thorax 7.0 MIP (b) Decrypted image with *EKEY* (c) Decrypted image with *EKEY*1 (d) Decrypted image with *EKEY*2 (e) Decrypted image with *EKEY*3 (f) Decrypted image with *EKEY*4 (g) Decrypted image with *EKEY*5 (h) Decrypted image with *EKEY*6.

and the mismatch key based on the same cipher image in the decryption processes, as shown in Table 9. Experimental test analysis shows that our proposed solution has high key sensitivity, whether it is in the encryption process or the decryption process, and can effectively resist brute force attacks.

G. SELECT PLAINTEXT/CIPHERTEXT ATTACK ANALYSIS

In our encryption algorithm, the encryption key is related to the information entropy of the approximation coefficients vector of the ROI, that is, the ciphertext is related to the plaintext, so our proposed algorithm model can effectively resist the select of plaintext/ciphertext attack.

H. NOISE AND CROPPING ATTACKS ANALYSIS

In the real world, the image transmission process may be subject to noise attacks, such as salt-and-pepper noise (SPN), Gaussian noise (GN), and speckle noise (SN), which may cause difficulties in image restoration [38]. If a cipher image can be successfully recovered from a noise attack, it means that the encryption algorithm has the ability to resist noise attacks.

In the experimental analysis, the "MRI image Brain" is used as the plain image, and its cipher image is shown in Fig.13(k). We performed noise attacks with different densities and variances on the cipher image and then decrypted the attacked images. The test results are shown in Fig.19. Fig19 (a)-(f) show cipher images attacked by different noises, and Fig19(g)-(l) are the recovery results of decrypted images corresponding to Fig19(a)-(f), respectively. To further quantitatively analyze the recovery degree of the decrypted image, we measured the PSNR between the plain image and the decrypted images after being attacked by noise. The results are listed in Table 10. As can be seen from Table 10, PSNR values are all greater than 46 dB, which means that our encryption algorithm can resist noise attacks to a certain extent.

TABLE 10. The PSNR between the plain images and the decrypted images in noise attacks.

Noise attack	PSNR
SPN 0.000005	50.0340
SPN 0.00001	46.5858
SN 0.000001	51.6745
SN 0.000003	51.6744
GN 0.02	51.6749
GN 0.0225	51.6743

In addition to noise attacks, cropping attacks are another means of attack on cipher images [43]. In our algorithm design, the encryption process does not need to transmit or embed the position information of the ROIs, and the decryption algorithm can automatically locate the ROIs. Therefore, if the cipher image is clipped, the ROI position

TABLE 11. Encryption speed comparison.

Image	Image Size	Full encryption	$\tau = 0$	$\tau = 23$	$\tau = 70$
Thorax 7.0 MIP	512×512	0.186s	0.150s	0.140s	0.120s
MRI image Brain	320×320	0.100s	0.111s	0.095s	0.080s
Ref. [44]	512×512	0.287s	–	–	–
Ref. [45]	512×512	1.26s	–	–	–

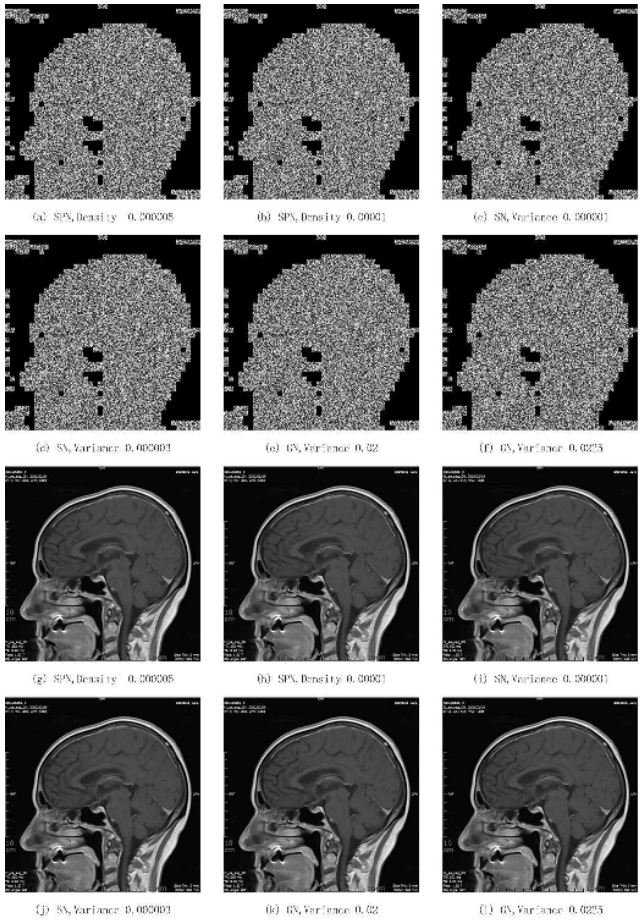

FIGURE 19. Noise attack analysis results; (a) is the noisy image under SPN and noise density = 0.000005 (b) is the noisy image under SPN and noise density = 0.00001 (c) is the noisy image under SN and noise variance = 0.000001 (d) is the noisy image under SN and noise variance = 0.000003 (e) is the noisy image under GN and noise variance = 0.02 (f) is the noisy image under GN and noise variance = 0.0225 (g)-(l) are the corresponding decrypted images of (a)-(f), respectively.

information hidden in the cipher image will be lost, making the cipher image unrecoverable.

What needs a special explanation here is that medical images contain very important pathological information of patients. Even a small-scale tampering and information loss occurs will seriously affect the diagnosis of doctors. Therefore, considering the security of medical image, we should try to avoid the attacks that damage the image information, such as noise attacks or cropping attacks, or start the corresponding warning strategy after such attacks, then correct and upload the image again to ensure the doctors get the lossless medical image.

TABLE 12. Decryption comparison of existing related frequency domain encryption schemes.

Algorithm	PSNR(dB)	SSIM
Ref. [32]	$35 \sim 40$	–
Ref. [31]	31	–
Ref. [33]	$50 \sim 60$	–
our(Thorax 7.0 MIP)	∞	1
our(Thorax 5.0 B31f)	∞	1
our(CT_SLICES)	∞	1
our(MRI image Brain)	∞	1

I. SPEED PERFORMANCE

In addition to the security of encryption algorithm, encryption speed is also an important indicator in the actual application process. The proposed scheme was implemented in MATLAB using a personal computer with Intel Core $i5 - 2450M$ 2.50 CPU and 8 GB of RAM. In Table 11, 512×512 and 320×320 medical images were respectively encrypted with full encryption and the proposed encryption scheme (i.e. Threshold $\tau = 0$, 23, and 70 respectively). Compared with other encryption algorithms, we can conclude that our proposed scheme meets the requirements of fast encryption. In addition, based on the game theory parameter optimization method described in Section 2, we can choose the optimal threshold according to different security requirements. The proposed scheme is more flexible and can be applied to real-time applications with different security levels.

J. LOSSLESS DECRYPTION ANALYSIS

Medical images contain patient information. If the medical image is detrimental to decryption, it will affect the doctor's diagnosis, which may lead to misdiagnosis and cause medical malpractice. Therefore, medical images should meet the requirements of lossless decryption. However, most of the current frequency domain encryption schemes cannot achieve lossless decryption. In our encryption scheme, we pioneered the lossless decryption after frequency domain encryption by changing the image structure.

We use PSNR and SSIM as evaluation indicators to evaluate whether the encryption algorithm achieves lossless decryption. PSNR is the most common and widely used image objective evaluation index. It is based on the error between corresponding pixel points, namely, the image quality evaluation based on error sensitivity. Because the visual characteristics of human eyes are not considered, the evaluation results are often inconsistent with people's subjective feelings. SSIM is also a fully referenced image quality

TABLE 13. Decryption comparison of existing related frequency domain encryption schemes.

Scheme	ROI Detection	Adaptive	Lossless Decryption	ROI position information
Ref. [32]	Manual	No	No	Transferred
Ref. [12]	Threshold Segmentation	No	Yes	Data Embedding
Ref. [23]	Manual	No	No	Data Embedding
Ref. [46]	Manual	No	No	Transferred
Ref. [15]	Salient Object Detection	Yes	Yes	Data embedding
Ref. [8]	Threshold Segmentation	No	Yes	Transferred
Ref. [17]	Face Detection	No	Yes	Transferred
The Proposed Scheme	Threshold Segmentation Based on Game Theory	Yes	Yes	Automatic locating

evaluation index, which measures the similarity of images in terms of brightness, contrast, and structure. If the image is lossless decrypted, the PSNR and SSIM between the decrypted image and the original image should be ∞ and 1, respectively. Table 12 illustrates the decryption comparison between the proposed scheme and existing related frequency domain encryption schemes. Experimental results show that the algorithm achieves lossless decryption and avoids medical accidents caused by the loss of decrypted image information.

K. COMPARISON WITH OTHER ROI SCHEMES

We compare our scheme and existing models from four aspects: ROI detection method, adaptive ability, lossless decryption ability, and ROI position information processing method, see Table 13. Firstly, the proposed scheme is an ROI selection encryption algorithm based on game optimization parameters, which can detect the ROI of medical images faster, more accurately, and more effectively. Secondly, this algorithm's ROI segmentation parameters are flexible and variable, so it can automatically adapt to images of different types and different formats. Then, because we adopted the method of image format conversion, the proposed algorithm realized lossless decryption. Furthermore, our algorithm can automatically locate the ROI, which further avoids the potential security risks of information leakage caused by the embedding or transmission of ROI position information.

V. CONCLUSION

In this paper, the ROI optimization lossless medical image encryption and decryption scheme based on game theory is proposed. The bargaining game is utilized to optimizes the ROI parameters. In this way, the ROI can be determined accurately and adaptively, which adapts multiple types of medical images and different encryption requirements. The encryption algorithm performs pixel-level image format conversion, realizes lossless decryption, and effectively protects the integrity of medical image information. Additionally, the encrypted ROI location information does not need to be processed separately, which can better reduce the risk of information leakage. Experiments and comparisons with other systems show that our scheme is suitable for the practical application of protecting medical image information because of its strong security, high flexibility, and fast speed.

REFERENCES

[1] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[2] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014.

[3] Ü. Çavu oğlu, S. Kaçar, A. Zengin, and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dyn.*, vol. 92, no. 4, pp. 1745–1759, Jun. 2018.

[4] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve El Gamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.

[5] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Cham, Switzerland: Springer, 2009.

[6] Z. Su, G. Zhang, and J. Jiang, "Multimedia security: A survey of chaos-based encryption technology," in *Multimedia—A Multidisciplinary Approach to Complex Issues*. Rijeka, Croatia: InTech, 2012, pp. 99–124.

[7] T. Xiang, S. Guo, and X. Li, "Perceptual visual security index based on edge and texture similarities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 951–963, May 2016.

[8] M. Noura, H. Noura, A. Chehab, M. M. Mansour, L. Sleem, and R. Couturier, "A dynamic approach for a lightweight and secure cipher for medical images," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 31397–31426, Dec. 2018.

[9] L. Yuan and T. Ebrahimi, "Image privacy protection with secure JPEG transmorphing," *IET Signal Process.*, vol. 11, no. 9, pp. 1031–1038, Aug. 2017.

[10] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Comput. Methods Programs Biomed.*, vol. 111, no. 3, pp. 662–675, Sep. 2013.

[11] N. A. Memon and S. A. M. Gilani, "Watermarking of chest CT scan medical images for content authentication," *Int. J. Comput. Math.*, vol. 88, no. 2, pp. 265–280, Jan. 2011.

[12] S. Zhang, T. Gao, and L. Gao, "A novel encryption frame for medical image with watermark based on hyperchaotic system," *Math. Problems Eng.*, vol. 2014, pp. 1–11, Apr. 2014.

[13] A. A. Abd El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," *Opt. Commun.*, vol. 285, nos. 21–22, pp. 4241–4251, Oct. 2012.

[14] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image information hiding algorithm that employs edge detection and data coding," *Comput. Methods Programs Biomed.*, vol. 127, pp. 24–43, Apr. 2016.

[15] J. Sun, X. Liao, X. Chen, and S. Guo, "Privacy-aware image encryption based on logistic map and data hiding," *Int. J. Bifurcation Chaos*, vol. 27, no. 5, May 2017, Art. no. 1750073.

[16] R. Bamal and S. S. Kasana, "Dual hybrid medical watermarking using Walsh-Slantlet transform," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 17899–17927, Jul. 2019.

[17] H.-W. Xue, J. Du, S.-L. Li, and W.-J. Ma, "Region of interest encryption for color images based on a hyperchaotic system with three positive Lyapunov exponets," *Opt. Laser Technol.*, vol. 106, pp. 506–516, Oct. 2018.

[18] R. Krishnamoorthi and P. Murali, "A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1217–1246, Jan. 2017.

[19] Z. Han, D. Niyato, and W. Saad, *Game Theory in Wireless and Communication Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[20] J. F. Nash, Jr., "The bargaining problem," *Econometrica, J. Econ. Soc.*, vol. 18, pp. 155–162, 1950.
[21] A. Muthoo, *Bargaining Theory with Applications*. Cambridge, U.K.: Cambridge Univ. Press, 1999.
[22] I. Ahmad and J. Luo, "On using game theory to optimize the rate control in video coding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 2, pp. 209–219, Feb. 2006.
[23] L. Li, A. A. Abd El-Latif, and X. Niu, "Elliptic curve El Gamal based homomorphic image encryption scheme for sharing secret images," *Signal Process.*, vol. 92, no. 4, pp. 1069–1078, Apr. 2012.
[24] Y. Liu, X. Qu, and G. Xin, "A ROI-based reversible data hiding scheme in encrypted medical images," *J. Vis. Commun. Image Represent.*, vol. 39, pp. 51–57, Aug. 2016.
[25] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Dec. 2018.
[26] J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677–1690, May 2017.
[27] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 2935–2945, Jul. 2020.
[28] X. Di, J. Li, H. Qi, L. Cong, and H. Yang, "A semi-symmetric image encryption scheme based on the function projective synchronization of two hyperchaotic systems," *PLoS ONE*, vol. 12, no. 9, Sep. 2017, Art. no. e0184586.
[29] L. Fortuna and D. Porto, "Quantum-CNN to generate nanoscale chaotic oscillators," *Int. J. Bifurcation Chaos*, vol. 14, no. 03, pp. 1085–1089, Mar. 2004, doi: 10.1142/S0218127404009624.
[30] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *Int. J. Bifurcation Chaos*, vol. 28, no. 01, Jan. 2018, Art. no. 1850010.
[31] N. Zhou, J. Yang, C. Tan, S. Pan, and Z. Zhou, "Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform," *Opt. Commun.*, vol. 354, pp. 112–121, Nov. 2015.
[32] J.-L. Liu, "Efficient selective encryption for JPEG 2000 images using private initial table," *Pattern Recognit.*, vol. 39, no. 8, pp. 1509–1517, Aug. 2006.
[33] E. A. Naeem, M. M. Abd Elnaby, N. F. Soliman, A. M. Abbas, O. S. Faragallah, N. Semary, M. M. Hadhoud, S. A. Alshebeili, and F. E. A. El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *J. Syst. Softw.*, vol. 97, pp. 118–127, Nov. 2014.
[34] N. Smart, S. Babbage, D. Catalano, C. Cid, B. D. Weger, O. Dunkelman, and M. Ward, "ECRYPT II yearly report on algorithms and keysizes (2011–2012)," in *Proc. Eur. Netw. Excellence Cryptol. (ECRYPT II)*, 2012, pp. 52–69.
[35] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[36] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[37] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[38] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on latin square and memristive chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 35419–35453, Dec. 2019.
[39] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
[40] Z.-H. Gan, X.-L. Chai, D.-J. Han, and Y.-R. Chen, "A chaotic image encryption algorithm based on 3-D bit-plane permutation," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7111–7130, Nov. 2019.
[41] L. Oteko Tresor and M. Sumbwanyambe, "A selective image encryption scheme based on 2D DWT, henon map and 4D qi hyper-chaos," *IEEE Access*, vol. 7, pp. 103463–103472, 2019.
[42] Y. Zhang, A. Chen, Y. Tang, J. Dang, and G. Wang, "Plaintext-related image encryption algorithm based on perceptron-like network," *Inf. Sci.*, vol. 526, pp. 180–202, Jul. 2020.
[43] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," in *Neural Computing and Applications*, no. 1. Springer, 2019, pp. 1–24.
[44] L. Liu and S. Miao, "A new simple one-dimensional chaotic map and its application for image encryption," *Multimedia Tools Appl.*, vol. 77, no. 16, pp. 21445–21462, Aug. 2018.
[45] X. Chai, Z. Gan, and M. Zhang, "A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion," *Multimedia Tools Appl.*, vol. 76, no. 14, pp. 15561–15585, Jul. 2017.
[46] D. Xiao, Q. Fu, T. Xiang, and Y. Zhang, "Chaotic image encryption of regions of interest," *Int. J. Bifurcation Chaos*, vol. 26, no. 11, Oct. 2016, Art. no. 1650193.

JIAN ZHOU received the B.S. degree in software engineering from the Binjiang College, Nanjing University of Information Engineering, in 2016. He is currently pursuing the master's degree in computer technology with the Changchun University of Science and Technology, China. His research interests include information security, chaotic systems, and image security.

JINQING LI received the B.S. degree from the Changchun University of Technology, in 2002, and the M.S. and Ph.D. degrees from the Changchun University of Science and Technology, in 2007 and 2014, respectively. She was a Visiting Scholar with Florida International University, from September 2018 to September 2019. She is currently an Associate Professor with the Changchun University of Science and Technology. Her major research interests include cyber security, information security, and chaotic encryption.

XIAOQIANG DI received the B.S. degree in computer science and technology and the M.S. and Ph.D. degrees in communication and information systems from the Changchun University of Science and Technology, in 2002, 2007, and 2014, respectively. He was a Visiting Scholar with the Norwegian University of Science and Technology, Norway, from August 2012 to August 2013. He is currently a Professor and a Ph.D. Supervisor with the Changchun University of Science and Technology. His major research interests include network information security and integrated networks.