AN ALGORITHM FOR REVERSIBLE INFORMATION HIDING OF ENCRYPTED MEDICAL IMAGES IN HOMOMORPHIC ENCRYPTED DOMAIN

XUEYAN WU*
School of Management, Guangdong University of Technology
Guangzhou 510520, China

ABSTRACT. At present, in reversible information hiding algorithm of image, the difference expansion idea is used. After the carrier image encryption, in encrypted image, information bits are embedded in the low value, resulting in the fact that in the image embedded with watermarking information, a part of the boundary pixel value has flipped. After being extracted, the carrier image cannot be recovered completely that is not only a large quantity of calculation, and the image quality has also been some damage. A algorithm for reversible information hiding of encrypted the medical image in the homomorphic encryption domain is proposed. Combining wavelet and fast fuzzy algorithm, the image edge is extracted from the high frequency and low frequency parts of medical image, and the medical image is reconstructed in the compressed boundary part. Combined with the thought of block compressed sensing and block edge pixels, the reconstructed medical image is divided to multiple non-overlapping blocks. The pixel in the right lower edge of the block is made homomorphic encryption operation, the remaining pixels are made compressed sensing operation, and the two parts are combined to a ciphertext to be sent to the owner of the channel According to the information hiding key the secret information is embedded into the ciphertext by the channel owners. The receiver can extract the information and restore the original image based on the encryption key and the information hiding key. The experimental results show that the proposed algorithm has high embedding capacity, the image quality after recovery is high, and the computational complexity is low.

1. Introduction. The development of computer network makes people all over the world that can exchange information anytime and anywhere, and this kind of communication is fast, convenient and cheap [5, 17]. In recent years, the way of information dissemination is more and more abundant. Because the digital image is easy to acquire, process, store and disseminate, so most multimedia data are based on digital image as carrier [8, 11]. However, data in the process of transmission, storage and processing are faced with security problems such as forgery, theft and illegal copying [2, 15]. Therefore, privacy protection, secret communication and information security are the urgent problems to be solved in the process of information transmission [6, 10]. Encryption technology is one of the effective ways to achieve secure transmission of medical image information. It transforms the protected medical image information into a form which is not understood by

2010 Mathematics Subject Classification. 43A35.
Key words and phrases. Homomorphic encrypted domain, encrypted medical image, reversible information hiding algorithm.
* Corresponding author: Xueyan Wu.

1441
people, so that the unauthorized party cannot get the image content to achieve the purpose of protecting image content [13, 21].

At present, domestic experts and scholars put forward many methods for reversible information hiding of medical image, such as image reversible data hiding algorithm based on threshold segmentation image reversible data hiding algorithm based on histogram modification image reversible information hiding algorithm based on diamond encoding [16]. Image’s reversible information hiding algorithm based on histogram modification mainly embeds information by modifying the most important point of original image histogram. Compared with most existing reversible hiding algorithms, the peak value of signal-to-noise ratio of watermark information embedded in image is high. But the embedding capacity is restricted by the maximum size of the histogram, which makes the embedding capacity limited to the original image [3, 12]. After the carrier image is encrypted by other two algorithms, in encrypted image, information bits are embedded in the low value, resulting in some block boundary pixels value in the image with watermark information has flipped, after being extracted image cannot be recovered completely, it not only has a large amount of calculation and but also the image quality has been some injury. A algorithm for reversible information hiding of encrypted the medical image in the homomorphic encryption domain is proposed. The work of this article is mainly embodied in the following aspects:

1. In the process of edge detection of medical images, most of the lesions in medical images are blurred image information, showing the characteristics of weak edge. Combining wavelet and fast fuzzy algorithm, image edges are extracted respectively in high frequency and low frequency parts of medical images. The membership function is used to complete the transformation from medical image to membership matrix quickly, and the inverse transformation from membership matrix to medical image which can detect more accurate.

2. The efficient secrecy of homomorphic cryptography is used to encrypt the medical image content and embed the necessary reversible information. Combined with the idea of block compression and separation of edge pixels, the reconstructed medical images are divided into multiple nonoverlapping blocks. A homomorphic encryption operation is performed on the pixels of the lower right edge, and the remaining pixels are made compressed sensing operations. And the two parts are fused, to form the ciphertext to send to the owner of the channel. According to the information hiding key, the channel owner embeds the secret information into the ciphertext [1, 20]. The receiver extracts the information and restores the original image based on the encryption key and the information hiding key. Simulation results show that the proposed algorithm has high embedding capacity, and the computational complexity is low.

2. Reversible information hiding algorithm for encrypted medical image in homomorphic encrypted domain based on image edge detection.

2.1. Medical image denoising method based on EMD. As a typical nonstationary signal, biomedical signals have strong background noise. An empirical mode decomposition (EMD) method is used to denoise medical images. The process of empirical mode decomposition can be understood as a screening process that takes the extreme feature scale of the image signal as a measure. The image signal is
screened from the smallest feature scale, and the intrinsic modal function of the shortest period is obtained. Through a layer of sieving, we can get multiple IMF with a gradual increase in the length of the cycle. This process also embodies the filtering process of multiresolution analysis of medical images. The space-time filter is based on the decomposition component IMF of the signal. Therefore, this filter fully preserves the non-linear and non-stationary characteristics of the signal itself. The specific steps of EMD applied to medical image denoising are as follows:

(1) A Gauss noise with a mean value of 0 and a variance of 0.01 is added to the original medical image.

(2) To extract each row (column) after image processing, it can decompose the image by EMD, to get the each modal function, and draw the function diagram [4]. The abscissa coordinate is the number of pixels, and the longitudinal coordinate is the gray values.

(3) To analyze and compare the decomposed modes, and to study the influence of each mode on the image.

(4) The high frequency information of each row (column) is decomposed, and the appropriate threshold is selected for the superposition of the low-frequency components after filtering.

(5) To analyze and compare the results of comparison between the medical image and the denoised image.

In the above test steps, the second step is the most important part of the whole algorithm. In particular, the selection of the threshold and the quantization of the threshold are related to the quality of the denoising of the image signal. The threshold function expression is:

\[
\hat{w}_{j,k} = \begin{cases} 
  \text{sgn}(w_{j,k}) \left| w_{j,k} - \frac{\lambda}{\exp\left[\frac{|w_{j,k} - \lambda|}{\sigma}\right]} \right|, & |w_{j,k}| \geq \lambda \\
  0, & |w_{j,k}| < \lambda
\end{cases} 
\]  

\[ \hat{w}_{j,k}' = \begin{cases} 
  \text{sgn}(w_{j,k}) \left| w_{j,k} - \frac{\lambda}{\exp\left[\frac{|w_{j,k} - \lambda|}{\sigma}\right]} \right|, & |w_{j,k}| \geq \lambda \\
  0, & |w_{j,k}| < \lambda
\end{cases} \tag{1}
\]

Where, \( N \) is an arbitrary normal number, and \( \lambda \) can be calculated according to the formula \( \beta \sigma \sqrt{2N} \), of which \( \beta \) is a correction factor and \( \sigma \) is a noise variance.

2.2. Medical image edge detection based on Wavelet and fast fuzzy algorithm. The edge detection algorithm is constructed by using the advantages of wavelet decomposition and fast fuzzy algorithm. In the fast fuzzy edge detection algorithm a simple membership function is used, which can quickly transform the image to the membership matrix and transform the membership matrix to the image, so that the useful information contained in the low-frequency signal after wavelet decomposition can be utilized. In order to preserve weak edges in medical images, in the use of wavelet modulus maxima edge detection based on the proposed fast fuzzy algorithm weak edge information can be extracted, and finally the application of multiscale edge fusion algorithm of edge image synthesis under different scale images is obtained. The specific process is as follows:

The function \( \theta(x) \) is called a smooth function, if \( \theta(x) = O(1/(1 + x^2)) \), and its integral is nonzero generally, the energy of the smooth function is usually concentrated in the low frequency section, so the smooth function can be regarded as the system influence function of the low pass filter [7]. Thus, the convolution \( (f \ast \theta)(x) \) of
\( f(x) \) and \( \theta(x) \) attenuates the high frequency information of \( f(x) \) without changing the low frequency part, thus smoothing the \( f(x) \). Taking:

\[
\begin{align*}
\psi_1(x) &= d\theta(x)/dx; \\
\psi_2(x) &= d^2\theta(x)/dx^2 \\
W^1f(s,x) &= f \cdot \psi_1^*_s(x); \quad W^2f(s,x) = f \cdot \psi_2^*_s(x)
\end{align*}
\]

Then

\[
\begin{align*}
\psi^1f(s,x) &= f \ast (sd\theta_s/dx)(x) = s \frac{d}{dx}(f \ast \theta_s)(x) \\
\psi^2f(s,x) &= f \ast (s^2d^2\theta_s/dx^2)(x) = s^2 \frac{d^2}{dx^2}(f \ast \theta_s)(x)
\end{align*}
\]  

(3)

The wavelet transform \( \psi^1f(s,x) \) and \( \psi^2f(s,x) \) are directly proportional to the first and two derivative of the function \( f(x) \) after being smoothed by \( \theta_s(x) \). The extreme point of the first derivative of the derivative corresponds to the zero point of the second derivative, and it is also the inflection point of the function \( f(x) \) itself. The maximum value of the absolute value of the first derivative corresponds to the mutation of the function, while the minimum value (not 0) corresponds to the slow change. In particular, if \( \theta(x) \) is a Gaussian function, the zero point detection is equivalent to the Marr-Hildreth edge detection, and the extreme point detection is corresponding to the Canny edge detection \[9, 18\]. When the scale of \( S \) is larger, the convolution with \( \theta_s(x) \) will eliminate the slight fluctuation of the signal, which can only detect the violent changes at the large structure. For the fixed scale \( s \), the local maximum point of \(|W^1f(s,x)|\) corresponds to the mutation point of \( f(x) \), and the zero crossing point of \( W^2f(s,x) \) corresponds to the turning point of \( f(x) \). If the wavelet function is selected as the first derivative of the smoothing function, the catastrophe point (singularity) of the signal can be detected by the maximum point of the absolute value of the wavelet transform \( W^1f(s,x) \). The modulus maxima of the wavelet transform should be at the point of mutation of the image. The edge point is a kind of mutation point of the image. Therefore, the edge of the image can be determined by detecting the modulus maxima point of the wavelet transform. Because the wavelet transform is located at every scale, the wavelet transform on each scale provides certain edge information, so it is called the multi-scale edge.

In the inverse transformation of \( \mu'_{ij} \), the gray value \( x'_{ij} \) of the pixel \((i,j)\) in the image \( X' \) after the fuzzy enhancement is:

\[
x'_{ij} = T^{-1}(\mu'_{ij})
\]

(4)

\( T^{-1}(\mu'_{ij}) \) is the inverse operation of \( T^{-1}(\cdot) \) in formula (9). Then the edge is extracted and the “min” or “max” operators are used \[14, 19\]. The edge matrix of the medical image using the next formula is as follows:

\[
E_{dge} = \bigcup_m \bigcup_n l^m_{mn}
\]

(5)

Where, \( l^m_{mn} = |l_{mn} - \min_R \{l^R_{mn}\} | \), \( R \) can be taken as a \( 3 \times 3 \) window centered on coordinate \((m,n)\).

2.3. Reversible information hiding algorithm for medical images based on block compression and homomorphic encryption. Supposing that \( \hat{M} \) is the pixel of a plaintext state in grayscale medical image. A RC4 random key stream \( K \) generated by the key seed \( S \) is selected to encrypt \( \hat{M} \) pixel by pixel, and get the
ciphertext $C$. In the next formula, $E()$ represents the encryption process, and $D()$ represents the decryption process. The encryption method is as follows:

$$C = E(M, K) = (M + K) \mod 256 = (m_\alpha + k_\alpha) \mod 256 = c_\alpha$$  

(6)

Where, the number of pixels in the original image is represented by $L$, and the $\alpha$th plaintext pixel, the random numbers in the key stream and the ciphertext pixels are represented by $m_\alpha$, $k_\alpha$ and $c_\alpha$, respectively. The decryption way is as follows:

$$D(C, K) = (c_\alpha - k_\alpha) \mod 256 = m_\alpha \mod 256$$  

(7)

Supposing that $X = \{x_1, \ldots, x_N\}$ is a discrete and uniformly distributed element set, so the probability $p(x_1) = p(x_N) = 1/N$ of each element can be gotten. If $X$ is divided by a general parser press according to the formula $X_L = D(X, L)$, and for $\forall T^L \in X_L$ and $\forall T^{L+1} \in X_L$, the information entropy of the tuples $I(T^L)$ and $I(T^{L+1})$ satisfies the following formula:

$$I(T^L) > I(T^{L+1})$$  

(8)

The above description indicates that the sum of the self information when the length of the output tuple is $L$ is greater than the synthesis of information when the length is $L + 1$, that is to say, $X_L$ has a greater information entropy to $X_{L+1}$. Since $X$ is fixed, the redundancy in the parsed signal can be eliminated in the form of entropy coding. It shows that the encrypted medical image information still has the entropy value that can be used.

2.4. Description of improved algorithm. In order to make better use of the information entropy of the encrypted medical image, the reversible information hiding algorithm of medical image based on block compression is improved. Combining the block compressed sensing and homomorphic encryption scheme, the black and white rectangular rectangles are the measurement coefficients of image block through measurement matrix observation. It is obvious that the coefficient of measurement is less than the amount of data in the original image block. The obtained observations are sent to the owner of the channel as ciphertext information.

(2) Information embedding. After receiving the observed values in Figure 1, information is hidden only in the measured values of the black rectangle. When the information 0 is embedded, no operation is done on the black rectangle; when the information 1 is embedded, all the observed values in the black rectangle are turned over by the formula.

$$y'_i = A \times 255 - y'_i$$  

(9)

Figure 1. coefficient of medical images after block compression perception processing
Where, \( y_i \) is the observed value of the \( i \) black rectangle. \( A \times 255 \) indicates the size as same as the observation matrix, the matrix is with a total element value of 255, and \( y'_i \) is the observed value after embedding information 1.

(3) Information extraction and image recovery. In the process of information hiding, for the overturned observation, the corresponding image block, which is decrypted, should be \( 255 - x_i \), that is, the value of all pixels in the block is opposite to 255, proved by the following formula.

\[
y'_i = A \times 255 - y'_i = A \times 255 - A \times x_i = A \times (255 - x_i) \tag{10}
\]

Because there is strong correlation between adjacent pixels of medical images, the value of the edge pixels of two adjacent unturned image blocks will be close, but for the unturned image blocks and the flipped image blocks, the difference of pixel values on their edges should be very large. Therefore, for the decrypted image with hidden information, it can use the edge pixels of the white blocks that are not embedded information (corresponding to the white dots in Figure 1) to evaluate whether the adjacent blocks (the black dots in the corresponding Figure 1) are overturned, that is, whether the embedded information is 1 or 0. The gradient value of the block boundary is calculated by using the formula (11), of which \( s \) represents the block size, and \( p_{0,v}, p_{s+1,v}, p_{s,v} \) and \( p_{u,s+1} \) fall into the adjacent blocks.

\[
f = \sum_{v=1}^{s} (|p_{1,v} - p_{0,v}| + |p_{s+1,v} - p_{s,v}|) + \sum_{u=1}^{s-1} (|p_{u,1} - p_{u,0}| + |p_{u,s+1} - p_{u,s}|) \tag{11}
\]

The medical image is first divided into two parts of \( I_1 \) and \( I_2 \) by the medical image owner. By using the encryption key \( K_{n1} \), the Gauss random measurement matrix is generated, the image \( I_1 \) is compressed and encrypted, \( I_{n1} \) is obtained, and another part of image \( I_2 \) is encrypted with the stream code \( K_{n2} \), to obtain the XOR encrypted image \( I_{n2} \). Then \( I_1 \) and \( I_2 \) are combined into the ciphertext medical image \( I_n \) to be sent to the information concealer. The information concealer uses the hidden key \( K_m \) to embed the secret information into the ciphertext medical image \( I_{n1} \), to obtain the medical image \( I_m \) containing hidden information. Finally, based on the encryption key \( K_{n1}, K_{n2}, \) and the hidden key \( K_m \), the medical image \( I_m \) containing secret information is processed by the recipient, to extract the secret information and restore the original medical image. The detailed description is as follows:

The original medical image is divided into the size of \( s \times s \) by the content owners, without overlap blocks, and then the lower right edge pixels of each image block are separated, as shown in Figure 2. The gray part represents the block right edge pixel

![Figure 2. grouping rules of medical image](image-url)
of the medical image, which is combined to the medical image $I_2$, the remaining is combined to the medical image $I_1$.

For medical image $I_1$, the block size is $(s - 1) \times (s - 1)$. Content owners use the encryption key $K_{n_1}$ to generate Gauss random measurement matrix $A'$. All blocks of medical image $I_1$ are observed using the same measurement matrix $A'$. Taking a block of $I_1$ as an example, $x_i \in \mathbb{R}^n(n = (s - 1) \times (s - 1))$ is the quantized results of $i$th piece of medical image block; if $y_i \in \mathbb{R}^m(m < n)(m = \text{compression rate} \times n$ represents a set of measurement coefficients of $x_i$), $y_i = A'x_i$, the measurement coefficients of each image block are combined, that is, the image $I_{n_1}$ after the block compression perception processing is obtained. Obviously, the plaintext content of the image $I_1$ after the BCS processing is kept confidential, and the amount of data after the encrypted image $I_{n_1}$ is also reduced than that of the plaintext image $I_1$. For the medical image $I_2$ in the homomorphic encrypted domain, a set of stream ciphers is generated by using the encryption key $K_{n_2}$. The image $I_2$ is encrypted with a stream cipher, and an exclusive or encrypted image $I_{n_2}$ is obtained. Finally, the content owner combines the medical images $I_{n_1}$ and $I_{n_2}$ into the ciphertext image $I_n$, which is sent to the information embedded person.

According to formula (21), in the process of information hiding, for the turned ciphertext blocks, the decrypted blocks should be $255 - x_i$, that is, all pixels in the block are opposite to 255.

After deciphering the medical images of the ciphertext, considering the correlation of medical images, the unflipped image blocks and the adjacent pixels that are not turned around should be smooth transition. For the turned image block, the value of the inner edge pixels of the block is different from that of the adjacent pixels that are not turned around, which should be larger. From Figure 2, we can see that white blocks are used to embed hidden information, while gray pixels around white blocks do not participate in information embedding. Therefore, combined with the unturned gray pixels around, we can see whether the white blocks are reversed through the following wave functions. According to the location of the image block, the wave function is expressed as follows:

The upper left corner image block is as:

$$f_1 = \sum_{v=1}^{s-1} |p_{s-1,v} - p_{s,v}| + \sum_{u=1}^{s-1} |p_{u,s-1} - p_{u,s}|$$  \hspace{1cm} (12)

The upper edge (except upper left corner) image block is as:

$$f_2 = \sum_{v=1}^{s-1} |p_{s-1,v} - p_{s,v}| + \sum_{u=1}^{s-1} |p_{u,1} - p_{u,0}| |p_{u,s-1} - p_{u,s}|$$  \hspace{1cm} (13)

The left edge (except the upper left corner) image block is as:

$$f_3 = \sum_{v=1}^{s-1} |p_{1,v} - p_{0,v}| + |p_{s-1,v} - p_{s,v}| + \sum_{u=1}^{s-1} |p_{u,s-1} - p_{u,s}|$$  \hspace{1cm} (14)

Other image blocks are as:

$$f_4 = \sum_{v=1}^{s-1} |p_{1,v} - p_{0,v}| + |p_{s-1,v} - p_{s,v}| + \sum_{u=1}^{s-1} |p_{u,1} - p_{u,0}| + |p_{u,s-1} - p_{u,s}|$$  \hspace{1cm} (15)

Where, $p_{0,v}, p_{s,v}, p_{u,0}$ and $p_{u,s}$ all fall in the image $I_2$. 
Once the receiver knows the combination method of the two parts of medical image \( I_m \) including secret information, the block size, encryption key \( K_{n2} \) and \( K_{n1} \), and the key \( K_m \) used for information hiding can restore the original medical image and extract the secret information.

3. **Experimental results and analysis.** In order to verify the comprehensive effectiveness of the reversible information hiding algorithm in the homomorphic encryption domain proposed in this paper, it needs to do an experiment and use matlab2010a to implement the algorithm. The test environment is Intel Core i3–3220CPU@3.30GHz, and multiple evaluation indexes are selected to compare the effectiveness of different algorithms for reversible information hiding of medical images.

(1) Mean square variance (MSE): MSE is the simplest measure of image quality. For an original medical gray image \( A \) with an image size of \( M \times N \), the image \( A' \) is obtained after embedding secret information in the medical image. Then, the degree of change of the image \( A' \) relative to the original image \( A \) can be evaluated by calculating the MSE between the pixels. The calculation formula of MSE is as follows:

\[
MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (A(i,j) - A'(i,j))
\]

(16)

Where, \( A(i,j) \) represent the pixel values of medical images, and \( A'(i,j) \) represents the pixel values of the medical images that carry the secret information, that is, the pixel value of the target medical image. \( M \) and \( N \) represent the height and width of medical images, respectively. It is known from the upper form that the image quality changes obviously when the calculated \( MSE \) values are large.

(2) The peak signal-to-noise ratio (PSNR): PSNR is an engineering term used to represent the ratio of the maximum possible power of a signal to the destructive noise power to express its accuracy. The unit of PSNR is dB. In general, high PSNR value indicates that the image distortion is low, and relatively low PSNR value indicates that the hidden secret information has the better invisibility, that is, after embedding the secret information, the medical image only changes slightly.

\[
PSNR = 10 \cdot \log_{10} \left( \frac{(2^k - 1) \times (2^k - 1)}{MSE} \right) = 10 \cdot \log_{10} \left( \frac{255^2}{MSE} \right)
\]

(17)

Since the pixel values of the medical gray level images are between 0 and 255, the value \( k \) is constant. The size of PSNR is affected by MSE. The smaller the MSE is, the larger the PSNR value is, indicating that the hidden secret information has the better invisibility, that is, after embedding the secret information, the medical image only changes slightly.

Firstly, the test results of the standard test medical gray image LE \((512 \times 512 \times 8\), as shown in Figure 3\) can prove the feasibility of the algorithm proposed in this paper. Figure 3 (a) shows the original medical gray scale image. Figure 3 (b) shows an encrypted medical image containing secret information with an embedding rate of 0.4833bpp. The recipient can decrypt the medical image directly according to the decryption key, and obtain the result of Figure 3 (c). It can be seen that the visual effect of the medical image is poor. For the decrypted medical images, interpolation technology can be used to reconstruct medical images appropriately, and we can get the result of Figure 3 (d) and extract the error free secret information.
It is known that the size of the initial medical image is $M \times N$, of which $M$ and $N$ are even. The number of pixels in all white positions in a medical image is marked as the number of lost pixels, as shown in Figure 1, and calculated using the next formula:

$$t = \frac{(N - 4) \times (M - 4)}{2}$$  \hspace{1cm} (18)
If \( M \) and \( N \) are large enough, the maximum embedding rate can be close to 0.6bpp. In fact, as the auxiliary information described in this article needs to be embedded in an encrypted medical image, a part of the embedded space is occupied. It is known that the size of the auxiliary information is \( s = b \times (\lceil \log_2 M \rceil + \lceil \log_2 M \rceil) + 32 \). In our experiment, all the test images are selected the standard gray scale of test medical image with the size of 512 \( \times \) 512 \( \times \) 8. Then the pure embedding rate is:

\[
\text{Pure embedding rate} = \frac{t - b - s}{M \times N} = 0.5 - \frac{2(M + N - 12) + 19 \times B}{M \times N}
\]

The location map is analyzed before comparing with other alternatives. The generation of location maps depends on the interpolation technique. Location map is a series of subsidiary information. It is used to tell whether a location of data embedding can be used to embed information, and at the same time, it is used to tell whether a location of the receiver can be embedded information. It is known that the auxiliary information consists of the size \( n'' \) of the secret information, the number of inlay pixels \( b \) in the white position and the location map \( L'' \). \( n'' \) and \( b \) only occupy 32bits, and the location map of the auxiliary information occupies the most part. Firstly, 8 standards to test medical images are tested. The number of that can not be used to be embedded in the position of white pixels in the eight standard test medical images is marked, as shown in Table 1. As you can see, the number \( b \) of pixels that are not embedded in the white position is smaller in general. But \( b \) of the two medical images of BA and BN, are larger than other medical images. This is mainly due to the large difference between the two medical images and the adjacent pixels, resulting in a larger map of the location.

The percentage of \( b \) in medical image embedding capacity is \( p \), that is:

\[
p = \frac{s}{t - b} \times 100\%
\]

Assuming that \( p < 100\% \), that is, \( s < t - b \) is established. It shows that the number of auxiliary information is less than the embedding capacity, and there are other spaces to use and embed secret information, so the algorithm is feasible. In fact, based on the characteristics of spatial correlation and interpolation of medical images, interpolation \( I' \) is very close to the original pixel value \( I \). As a result, it can be guaranteed that \( b \) is less than \( t \) (as shown in Table 1), and \( s \) is obviously less than \( t \). In the experiment, eight medical images are tested, and their maximum embedding rate and maximum pure embedding rate are obtained, as shown in Table 2. It can be seen from Table 2 that the maximum embedding rate is close to 0.5bpp. In the reversible information hiding algorithm based on threshold partition and the reversible information hiding algorithm based on histogram modification, the embedding rate is determined by chunking, and the larger the block is, the lower the embedding rate is. When the minimum block size is 4 \( \times \) 4, the maximum embedding rate is 0.0584bpp. The embedding rate of the image reversible information hiding algorithm based on rhombus coding can be controlled by different
variables. But the different embedding rate affects the reversibility. In the experimental data, we can see that to ensure completely reversible, that is, the error free recovery, the maximum embedding rate can reach 0.0857bpp. Both are far less than the embedding rate we can reach.

From table 2, we can find that although the number \( b \) of inlay pixels of each image is different, the maximum embedding rate has little different. This is because the total number of pixels in the image is far greater than \( b \). In addition, the maximum pure embedding rate is determined by the size of the auxiliary information. The more the auxiliary information is, the lower the pure embedding rate is, and on the contrary, the higher the pure embedding rate is. Table 2 shows that the pure embedding rates of Figures Barbara and Baboon are lower than that of other images, and it is precisely because of that these two images have greater auxiliary information than other images. Finally, we can find that all the pure embedding rate and the embedding rate are quite close. It shows that the auxiliary information does not have a great impact on the embedded capacity. As shown in Table 2, the auxiliary information only occupies a very small embedded space.

The proposed method, the reversible information hiding algorithm of image based on threshold segmentation (KF), the algorithm based on histogram modification (ZF), and the algorithm based on diamond coding (LO) are compared and the experimental data is to visually display the analysis results. It needs to be explained that the best situation in the literature is to be selected, that is, the lowest error rate. The three images of LE, AI and BA are analyzed, and the performance of three kinds of data, such as the error rate of data extraction, the PSNR of direct decryption image, and the PSNR of recovery image, are analyzed, as shown in Table 3 to 5. For the proposed method, there are two values in the PSNR column of the direct decryption image. The first value is the PSNR of the direct decryption image, and the second value is the PSNR value of the image restored by the interpolation technology for the direct decryption image.

As for the data extraction error rate, the mean variance calculation results can be as the reference. As mentioned above, the algorithm can extract all the secret information exactly. In the KF algorithm and LO algorithm, the smaller the block is, the higher the error rate is. The quality of the image is described by the value of PSNR. First of all, for the direct decryption of the image, in the proposed algorithm, the quality of direct decryption image containing secret information is very low, because the MSB is turned over. We can reconstruct the image by using the interpolation technique as a filter to improve the PSNR value of the image. The results after filtering are better than other algorithms. While in the KF algorithm.

### Table 2. maximum embedding rate and maximum pure embedding rate of eight test images

|       | LE   | AI   | BA   | BN   | BO   | HI   | PE   | LA   |
|-------|------|------|------|------|------|------|------|------|
| Maximum embedding rate/bpp | 0.4855 | 0.4855 | 0.4802 | 0.4812 | 0.4855 | 0.4932 | 0.4932 |
| Maximum embedding rate/bpp | 0.4854 | 0.4852 | 0.4525 | 0.4758 | 0.4825 | 0.4821 | 0.4921 | 0.4924 |
and ZF algorithm, it can be achieved by embedding three LSB of the pixels. The PSNR of the decrypted image can be approximately 36.25dB. For the LO algorithm, different variables have different PSNR, and the higher the embedding rate is, the worse the direct decryption image is. Finally, in view of the quality of the restored image, the proposed algorithm is completely reversible, and the image can be recovered without distortion, but other reversible algorithms can not be guaranteed. It can be seen that the proposed algorithm is superior to other algorithms.
Finally, we test the computational complexity of different algorithms. The test environment is the same as the above test environment. The experimental analysis is based on three main steps: how to distribute the complexity of medical image encryption, information embedding and recovery, and the result is shown in Figure 4. These three steps correspond to three operating subjects: the content owner, the data embed person and the recipient. The test time stipulates that all embeddable points can be used for embedding. That is to say, when testing embedding capacity reaches the maximum, recovery steps include receiver operation, data extraction and image recovery after decryption of medical images, and Figure 4 shows the average time of medical image LE. It can be clearly seen that the time spent in the step of secret information embedding is the least, which indicates that the load of data embed is the smallest in the reversible information hiding process of the whole medical image. Therefore, the reversible information hiding algorithm proposed in this paper is very ideal for the third party service providers who want to encrypt the medical image, because the main task of the third party service providers is to push data encryption into embedded.

4. Conclusions. Reversible information hiding technology for ciphertext domain combines encryption mechanism and reversible information hiding technology. It can play an irreplaceable role in the field of medical applications. Sometimes the content owner of data and the third party data manager are not the same person. Content owners do not want their information content to be known except for legal recipients. Therefore, it will firstly encrypt their information content, enabling data managers to embed effective information without knowing the plaintext of the data, but also in the data receiving end, they can extract effective embedding information and completely recover the carrier image, here, the reversible information hiding of encryption domain can be applied. In this paper, the reversible information hiding technology of image is studied in the plaintext and ciphertext domain. The multiple parts of the focus in medical images are blurred image information, showing the characteristics of the weak edge characteristics. To this end, Combining wavelet and fast fuzzy algorithm, image edges are extracted respectively in high frequency and low frequency parts of medical images. The membership function is used to complete the transformation from medical image to membership matrix quickly, and the inverse transformation from membership matrix to medical image, which can detect more accurate and clear edge images. The entropy of the homomorphic encryption and the image encryption are analyzed respectively. The encryption technology and the reversible information hiding technology are well combined, and the effectiveness of the algorithm is verified by experiments.
Acknowledgments. Youth Fund for the Humanities and Social Sciences of the Ministry of Education: Customer Engagement Behavior in Social Media Environment (No. 13YJCZH200).

REFERENCES

[1] M. A. Akhaee, S. M. E. Sahraeian, B. Sankur and F. Marvasti, Information hiding with maximum likelihood detector for correlated signals, IEEE Transactions on Multimedia, 36 (2015), 144–155.
[2] M. Aziz, M. H. Tayarani-N and M. Afsar, A cycling chaos-based cryptic-free algorithm for image steganography, Nonlinear Dynamics, 80 (2015), 1271–1290.
[3] B. Bank, J. Heintz, G. Matera, J. L. Montana, L. M. Pardo and A. R. Paredes, Quiz games as a model for information hiding, Journal of Complexity, 34 (2016), 1–29.
[4] A. Basu, K. Nandy, A. Banerjee, S. Giri, S. Sarkar and S. K. Sarkar, On the implementation of ip protection using biometrics based information hiding and firewall, International Journal of Electronics, 103 (2016), 177–194.
[5] H. Chen, J. Ni, W. Hong and T. S. Chen, Reversible data hiding with contrast enhancement using adaptive histogram shifting and pixel value ordering, Information Sciences, 250–265.
[6] K. Dong, H. J. Kim, S. C. Yong, H. J. Sang and B. H. Chung, Reversible binary image watermarking method using overlapping pattern substitution, Etri Journal, 37 (2015), 990–1000.
[7] W. F., W. L. and W. T. T, Hidden optimization algorithm simulation analysis of large capacity images, Computer Simulation, 3 (2016), 409–412.
[8] N. Jiang, N. Zhao and L. Wang, Lab based quantum image steganography algorithm, International Journal of Theoretical Physics, 55 (2016), 3722–3736.
[9] H. J. L and Z. X. H, Adjustable reversible data hiding algorithm with large embedded capacity based on image gradient prediction, Journal of Jilin University (Engineering and Technology Edition), 2074–2079.
[10] M. Li, D. Xiao, A. Kulsoom and Y. Zhang, Improved reversible data hiding for encrypted images using full embedding strategy, Electronics Letters, 51 (2015), 690–691.
[11] T. Luo, G. Jiang, M. Yu, H. Xu and F. Shao, Inter-view local texture analysis based stereo image reversible data hiding, Digital Signal Processing, 48 (2016), 116–129.
[12] K. Martin and K. Shankar, How often should you clean your room?, Discrete Mathematics and Theoretical Computer Science, 17 (2015), 413–441.
[13] Z. Qian, H. Zhou, W. Zhang and X. Zhang, Comments on Steganography Using Reversible Texture Synthesis, 4, IEEE Transactions on Image Processing, 2017.
[14] S. S. H., Ubiquitous data gathering algorithm based on maximization of information gain in wireless sensor networks, in Journal of China Academy of Electronics and Information Technology, 4 (2017), 371–377.
[15] L. B. Si and H. Y. Qiao, Evaluation of technological innovation efficiency in equipment manufacturing industry based on input orientation–panel data analysis based on data envelopment model, Journal of Discrete Mathematical Sciences & Cryptography, 20 (2017), 1381–1386.
[16] H. Unno, R. Yamkum, C. Bunporn and K. Uehira, A new displaying technology for information hiding using temporally brightness modulated pattern, IEEE Transactions on Industry Applications, 53 (2017), 596–601.
[17] C. Y. Wang, L. Li, H. R. Li, C. L Qin and H. Y. Zhao, Research on the digital image encryption algorithm based on double chaos, Bulletin of Science and Technology, 12 (2016), 169–173.
[18] Y. J. Wang Dong—Chen, Knowledge management of web financial reporting in human-computer interactive perspective., Eurasia Journal of Mathematics Science & Technology Education, 13 (2017), 3349–3373.
[19] L. Yong, S. Tuo and J. Shi, Sparse solution of some special optimization problems, of Interdisciplinary Mathematics, 20 (2017), 595–602.
[20] X. Y. Zhang and J. Q. Wang, Consensus-based framework to mcgdm under multi-granular uncertain linguistic environment, Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 33 (2017), 1263–1274.
[21] H. Zheng, Y. Yang, D. Xiao and J. He, Rdh in bcs images based on block edge pixel separation, Electronics Letters, 53 (2016), 18–20.

Received June 2017; revised November 2017.

E-mail address: girl_ups@163.com