

Research Article

Medical Image Key Area Protection Scheme Based on QR Code and Reversible Data Hiding

Zelin Zhang ¹, Jian Xu ², Bin Ma ¹, Chunpeng Wang ¹, Jian Li ¹ and Yuli Wang ¹

¹Qilu University of Technology (Shandong Academy of Sciences),
Shandong Computer Science Center (National Supercomputer Center in Jinan),
Shandong Provincial Key Laboratory of Computer Networks, Jinan, China

²Shandong University of Finance and Economic, Jinan, China

Correspondence should be addressed to Bin Ma; sddxmb@126.com and Yuli Wang; wyl@qlu.edu.cn

Received 20 January 2021; Accepted 19 June 2021; Published 15 July 2021

Academic Editor: M.A. Jabbar

Copyright © 2021 Zelin Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Medical image data, like most patient information, has high requirements for privacy and confidentiality. To improve the security of medical image transmission within the open network, we proposed a medical image key area protection algorithm based on reversible data hiding. First, the coefficient of variation is used to identify the key area, that is, the lesion area of the image. Then, the other regions are divided into blocks to analyze the texture complexity. Next, we propose a new reversible data hiding algorithm, which embeds the content of the key area into the high-texture regions. On this basis, a quick response (QR) code is generated using the ciphertext of the basic image information to replace the original lesion area. Experimental results show that this method can not only safely transmit sensitive patient information by hiding the content of the lesion, it can also store copyright information through QR code and achieve accurate image retrieval.

1. Introduction

In recent years, with the rapid development of multimedia technology, medical imaging research has made great progress. Medical images have become an indispensable and effective auxiliary means for modern medical diagnosis. More and more hospitals and medical research institutions have established their own medical care system. The medical care system is used for image archiving and information transfer. However, the sharing and openness of the network exposes the transmission of medical images to danger. Usually, problems such as illegal copying, content tampering, and copyright loss are encountered, which greatly hinders the diagnosis of medical images. Therefore, researchers have invested more efforts in medical image security research, in which information hiding and image encryption [1–3] are two key research directions.

Information hiding technology embeds information that needs to be protected into a carrier. Usually, the carrier after extracting the secret information inevitably exhibits a certain

degree of distortion. However, special carriers such as medical images have extremely high requirements for image integrity, so reversible data hiding (RDH) technology is introduced to protect highly sensitive images. Reversible data hiding is an important branch in the field of information hiding. Reversible data hiding (RDH) embeds secret information into the carrier data and can completely extract the secret information and lossless recover the carrier data. In 1997, Barton [4] proposed the concept of reversible data hiding. Later, a large number of reversible data hiding schemes were proposed [5–7]. At present, reversible data hiding technology mainly includes lossless compression, difference expansion (DE), and histogram shifting (HS). Celik et al. [8] proposed a reversible data hiding scheme based on compression, embedding secret data into the redundant space generated by lossless image compression. This method has low computational complexity, but low embedding capacity and large image distortion. In 2003, Tian [9] proposed a reversible data hiding algorithm based on difference expansion, which extended the difference of

two adjacent pixels to embed the data into the vacant least-significant bit. Ni et al. [10] first proposed a reversible data hiding algorithm based on histogram shifting. This algorithm constructs a histogram based on the pixel distribution of the original image and embeds information through histogram shifting. This method has high efficiency, enhanced data embedding ability, and nondestructive recovery, which is suitable for medical image. On this basis, Kumar et al. [11] proposed an improved histogram shifting reversible medical image watermarking algorithm to improve the hiding capacity. It is based on histogram shifting technology to divide the image into smaller blocks for data embedding. Wu et al. [12] proposed an approach based on histogram shifting to protect medical image records. The linear predictor with nonuniform weight and threshold is used to improve the quality of medical image, and the prediction accuracy and embedding capacity are improved by adjusting the weight. Due to the reversibility of reversible data hiding algorithm, it is of great practical significance to protect medical images by using reversible data hiding technology. As mentioned above, most of the protection algorithms dealing with medical images mainly involve image copyright protection and embedded image visual quality enhancement. The security of image content itself is generally difficult to achieve. Therefore, in order to protect the change of image content (and any accidental leakage it may bring), most medical images are encrypted during transmission and storage.

Encryption technology achieves the function of hiding information by encoding information. Abdmouleh et al. [13] proposed a new approach of partial encryption based on the discrete wavelet transform (DWT) and compatible with the norm JPEG2000 in order to assure an optimal and a secure transmission and storage of medical images. Shalaby et al. [14] proposed a novel chaotic-based medical image encryption technique. This technique uses first a Butterworth high-pass filter (BHPF) to enhance the medical image's details to avoid any possible loss of medical details during the encryption-decryption process. The proposed technique is then developed by modifying Arnold's cat map technique combined with the well-known Advanced Encryption Standard (AES) algorithm. Zhou et al. [15] proposed a novel lossless medical image encryption scheme based on game theory with optimized the region of interest (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. 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.

But the above secret technology also has its own limitations. Firstly, in order to ensure lossless recovery of the image, the partial encryption technology will add additional coding. In addition, there may be problems in retrieving images in open networks, unless there is additional

nonencrypted information that can be accessed (which may damage some protection work) and the mechanism that only authorized medical personnel can decrypt the information. Moreover, the encrypted image is easy to attract the attention of attackers, which increases the risk of data being attacked.

In order to protect the privacy information of medical image, a key area protection algorithm based on QR code and reversible data hiding is proposed. Firstly, the key area of the image is located, which contains important pathological features or diagnosis and treatment information; then, the other areas of the image are processed in blocks, and calculate and sort the mean squared error (MSE) of image blocks, select high-texture region embedding, embed secret information by using histogram shifting technique, and realize the key information hiding; generate QR code according to medical image and patient information and replace the key area with a position change method. Finally, achieve the protection of medical image copyrights and patient information.

The structure of the article is as follows. The second part shows the histogram shifting algorithm and QR code technology. The third and fourth parts describe the algorithm flow. The fifth part discusses the performance of the algorithm. Finally, the conclusion is given in the sixth part.

2. Related Work

2.1. Histogram Shifting. Reversible data hiding schemes [10] based on histogram shifting have attracted wide attention due to their low computational complexity and high image quality. The histogram is generated by counting the pixel value information. The information is embedded by modifying the pixel value information. The main steps are as follows:

- (1) Generate the grayscale histogram of the original image (gray histogram shows the number of times the pixel value of the image appears, i.e., the frequency of the pixel), find the peak point P and zero point Z , and store the peak point and zero point information as auxiliary information.
- (2) Traverse the whole image, scan from top to bottom in sequence, and scan from left to right in column by column. The pixel between Z and P is shifted toward the Z by one unit, and the gray histogram next to the P is vacated to create a space for embedding secret information. h represents the original pixel value and h' represents the shifted pixel value:

$$h' = \begin{cases} 0, & h = P + 1, \\ h + 1, & P \leq h < Z, \\ h - 1, & Z < h \leq P. \end{cases} \quad (1)$$

- (3) Scan images in the same order. If the pixel value is equal to the peak pixel value P , then embed secret information. If it moves to the right, if the information bit to be embedded is "1," the pixel value increases by 1, and the pixel value changes to $P + 1$. If

the information bit to be embedded is “0,” the pixel value remains unchanged and remains P . b represents the secret information to be embedded, and the pixel value after embedding the secret information is expressed as

$$h' = \begin{cases} P, & b = 0, \\ P + 1, & b = 1 \&\& P \leq h \leq Z, \\ P - 1, & b = 1 \&\& Z \leq h \leq P. \end{cases} \quad (2)$$

The purpose of this method to find the peak point is to increase the embedding capacity as much as possible. In this algorithm, the embedding capacity is equal to the number of peak point P :

$$\text{capacity} = h(P). \quad (3)$$

2.2. QR Code. Since the 1980s, QR code has been applied on a large scale because of its low cost, fast identification speed, strong error correction ability, and other advantages. The widespread popularity of mobile phones and electronic devices also provides a suitable environment for the development of QR code. QR code is also known as Quick Response code [16]; full name is Quick Response code. It was developed by a Japanese company in 1994 for the tracking of automobile parts and has since been used in various fields. From the point of view of storage information, QR code can not only contain text information, but also jump directly to the interface of other websites through links, which can store a variety of types of data. From the appearance, the QR code is composed of black and white blocks divided into functional areas and coding areas. Compared with other 2D barcodes, QR code has the advantages of larger storage capacity, fast recognition speed, strong antistain ability, encryption and anticounterfeiting, etc., making it the most popular 2D barcode [17]. The algorithm uses QR codes to provide medical images and patient information. Nowadays, image retrieval is based primarily on external labels. If external labels are tampered with maliciously, it will lead to retrieval errors.

In this paper, image-related attribute information is in addition to the QR code. By scanning QR code information and comparing the corresponding keywords, the image can be quickly retrieved and the retrieval accuracy can be improved. The QR code contains basic information such as hospital information, department information, doctor information, patient number, image shooting time, contact number, and medical image type. The QR code generation function is asked to generate the QR code by using these information. It is convenient for content retrieval and copyright authentication of medical images and the disclosure of patient information and protects the copyright and patient information of medical images. In Figure 1(a) shows the basic information of the image and Figure 1(b) shows the QR code generated by the information.

3. Algorithm Description

In recent years, more and more hospitals and medical research institutions have established their own medical systems for image archiving and information transmission. However, relevant studies show that the systems used by most hospitals or medical research institutions are not secure and are vulnerable to attacks by illegal personnel leading to disclosure of patient information. Therefore, it is very important to protect the medical image. Based on the above reasons, this paper proposes a reversible data hiding-based medical image key information protection scheme [18].

3.1. Selection of Key Area. This section is a detailed introduction to Step 1 of Embedding Algorithm section. For ordinary medical images, the key area is the disease sign region, which contains important pathological features or diagnosis and treatment information. This region has rich texture and high information content. The other part has low texture, contains less information, and does not contain the key information of the image [19]. According to the characteristics of medical image information distribution, the effective information intensive area is selected as the key area to encrypt and realize the protection of medical image content. First, determine the size of the key area. For a medical image of 512×512 , if the number of pixels with a gray value of 255 is less than two-thirds of the total, the size of the key area is 128×128 ; otherwise, the size of the key area is 80×80 . Then, the location of the key area is determined. Coefficient of variation is usually used to calculate the degree of dispersion between data. The larger the coefficient of variation is, the higher the degree of dispersion of data is, and the more abundant the data is; the smaller the coefficient of variation is, the gentler the data changes and the less information content. The distribution of image pixel value is between 0 and 255, which also meets the calculation condition of coefficient of variation. According to the following equation, the coefficient of variation, which represents the standard deviation, is the population mean:

$$C_v = \frac{\sigma}{\mu}. \quad (4)$$

Equation (5) is used to calculate the standard deviation, N represents the total number of pixels in pixel blocks, x is the pixel value, and μ represents the population mean:

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - \mu)^2}. \quad (5)$$

The values of all subblocks were calculated and sorted. In order to verify the influence of coefficient of variation on the selection of key areas, three image blocks were selected and marked as $P1$, $P2$, and $P3$, respectively. $P1$ denotes the image block with the smallest discrete coefficient, $P2$ denotes the image block with the largest discrete coefficient, and $P3$ denotes the mean value of $P1$ and $P2$ and is rounded downward:

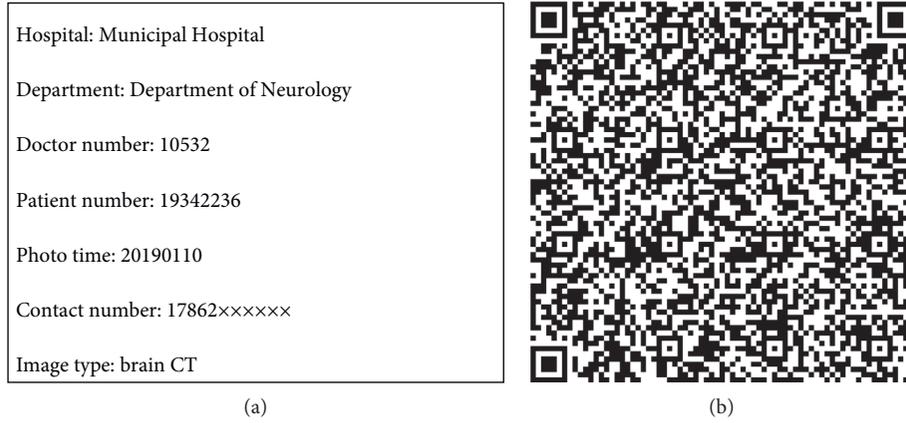


FIGURE 1: Generation of QR code. (a) Picture basic information. (b) Generated QR code.

$$\begin{cases} P1 = B_{\min}(C_v), \\ P2 = B_{\max}(C_v), \\ P3 = \lfloor P1 + P2 \rfloor. \end{cases} \quad (6)$$

According to equation (6), the key areas of the image are obtained, and then the key areas are embedded into the image as secret information.

3.2. Block Scheme. This section is a detailed introduction to Step 3 of Embedding Algorithm section. Based on the characteristics of medical image information distribution, non-overlapping block processing is generally adopted for medical image, which can increase the accuracy of calculation [20]. Assume that the original image is a grayscale image of size, M is the row of the image, N is the column of the image, and the size of each subblock is $n \times m$. According to the following equation, the original image is divided into K subblocks:

$$K = \left\lfloor \frac{N \times M}{n \times m} \right\rfloor. \quad (7)$$

3.3. Embedded Region Selection Scheme. This section is a detailed introduction to Step 4 of Embedding Algorithm section. For medical images, texture regions contain more information than smooth regions. The image distortion caused by secret information embedding can protect medical image information to a certain extent. Therefore, when selecting the embedding region, the texture region is preferred as the embedding region. The mean square error (MSE) can evaluate the texture degree of the image, so this scheme uses MSE to calculate the texture complexity of the image. The MSE calculation formula is as follows. m and n , respectively, represent the rows and columns of the image, $I(i, j)$ is the original image, and I_{ave} is the average pixel value of the image block:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - I_{ave}(i, j)]^2. \quad (8)$$

The MSE of each subblock of the image is calculated according to equation (8). The MSE is sorted from small to large according to the position of the corresponding image block, and the sequential sequence of MSE is obtained by using the sorting algorithm. Set the threshold value T to control the selection of embedded pixel value. When T increases, the number of pixels available for embedding will increase, but the image visual quality will decrease. In order to maintain the balance between embedding capacity and visual quality, it is necessary to set T reasonably.

During the data embedding phase, the texture region used for data embedding can be easily identified during the data extraction phase, as the change in the texture region's pixel value further amplifies the MSE of the selected block. Suppose the threshold value of texture and smooth block classification is set to 10. Then, all blocks with MSE greater than 10 participate in reversible data embedding, and after data embedding, the MSE of the selected block is further expanded. During the data extraction phase, the same threshold can be used to distinguish the blocks so that the secret message can be completely extracted.

4. Embedding and Extraction Schemes

Figure 2 shows the basic process of embedding this algorithm.

4.1. Embedding Algorithm

Step 1. The key areas of the image are selected by using the key area selection method in Section 3.1, and the key areas are transformed into binary streams and embedded into the image as secret information.

Step 2. Generate a QR code containing carrier image information as a visible watermark. The size of the QR code is consistent with the size of the key area. After that, the key area is replaced by the method of position exchange to generate the merged image.

Step 3. Divide other image regions into blocks according to the image partitioning method in Section 3.2.

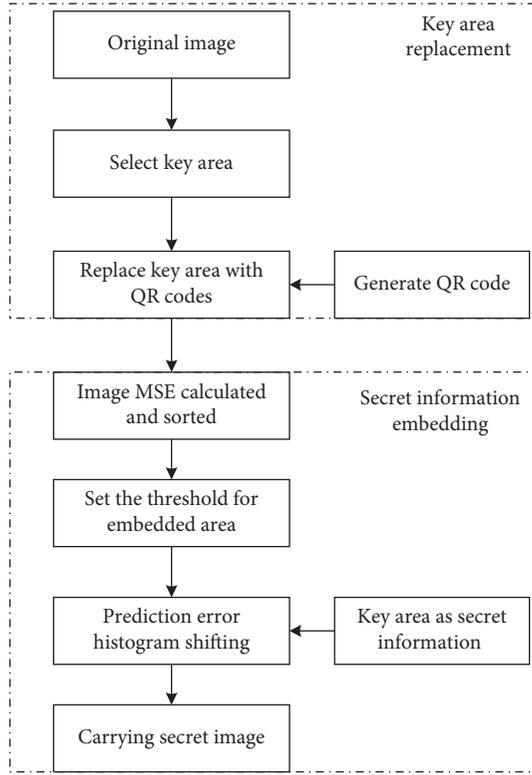


FIGURE 2: Flowchart of the basic process of embedding this algorithm.

Step 4. Calculate the MSE value of each image block and sort it from small to large. Set the threshold value T to divide the texture area and smooth area. Where MSE value is greater than T , it belongs to the texture region, which is regarded as embeddable region. The smooth area is taken as the nonembeddable area, and the QR code area is merged into the nonembeddable area.

Step 5. Scan each embeddable area image block from top to bottom and left to right in order to determine the embeddable order.

Step 6. Carry out diamond prediction for each embedded region image block based on embedding order [21]. Four adjacent pixels around each pixel are used to achieve the prediction of target pixel, and the predicted value is subtracted from the original pixel value to achieve the prediction error [22, 23]. Embed the odd layer first and then the even layer. The predicted value and prediction error are obtained through the following equation:

$$\begin{cases} u_{i,j} = \frac{v_{i,j-1} + v_{i,j+1} + v_{i-1,j} + v_{i+1,j}}{4}, \\ d_{i,j} = \lfloor u_{i,j} - v_{i,j} \rfloor. \end{cases} \quad (9)$$

Step 7. Generate the prediction error histogram of each image block, select the pixel point with the prediction error of $[-3, 3]$ as the embedding point, translate to get

the embedding space, and embed the secret information. The formula is as follows, where $[p, q]$ represents the error selection range, b represents the secret information:

$$D_{i,j} = \begin{cases} 2d_{i,j} + b, & d_{i,j} \in [p, q], \\ d_{i,j} + q + 1, & d_{i,j} > q, \\ d_{i,j} + p, & d_{i,j} < p. \end{cases} \quad (10)$$

4.2. Extraction Algorithm

Step 1. Select the QR code area (scan the QR code to get the basic information of the image).

Step 2. Divide the image into blocks according to the scheme when embedding.

Step 3. Calculate the MSE of each image block, sort from small to large, and select the texture area and smooth area according to the threshold value T . Where the MSE value is greater than T , it belongs to the texture area, and the QR code area is incorporated into the nonembeddable area.

Step 4. Based on the embedding order, the diamond shape prediction is made for each embedded region image block. First, the even-numbered layer is predicted and then the odd-numbered layer is predicted. The following equation is used to extract the secret information:

$$b = D_{i,j} \bmod 2. \quad (11)$$

Step 5. Generate the prediction error histogram of each image block, and use the following equation to restore the image by translation:

$$d_{i,j} = \begin{cases} \lfloor \frac{D_{i,j}}{2} \rfloor, & d_{i,j} \in [2p, 2q + 1], \\ D_{i,j} - q - 1, & d_{i,j} > 2q + 1, \\ D_{i,j} - p, & d_{i,j} < 2p. \end{cases} \quad (12)$$

Step 6. Reorganize the extracted secret information and restore it into image blocks, and replace the QR code area with the image blocks to restore the original image.

5. Experimental Results and Analysis

The experimental environment of this experiment is MATLAB 2016A, Intel® Core™ I7-6700 CPU processor. In order to evaluate the performance of the experimental scheme, we experimented with data from the cancer imaging archive (TCIA) medical imaging database. TCIA is an open-access database of medical images for cancer research. We manually selected 200 images from TCIA using the following selection modes: (a) images must describe common CT imaging organs, such as brain, lung, etc. (b) The

requirement of image texture is quite complex. Figure 3 shows 6 images showing different types of medical images [24]. The covered QR code image differs greatly from the original image. In order to ensure the reliability of the calculation results, the experimental data are the calculation results excluding the QR code part.

After embedding information, the load image is different from the original image. In order to prevent the change from being detected, the traditional reversible data hiding algorithm needs to ensure that the human eye cannot capture the change of the secret image. In this algorithm, we use the original image and the load difference in the secret image to protect the image content, because the medical image has high sensitivity, small changes can cause the wrong diagnosis; we use the embedded image distortion after image protection. Peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) are generally used to evaluate the visual quality of loaded images. In this study, the PSNR and SSIM between the embedded watermark image and the original image (excluding the QR code area) are calculated to objectively evaluate the image quality. The camouflage of human eye vision is mainly embedded part in the algorithm.

The larger the PSNR value is, the smaller the change of visual quality and the smaller the distortion after embedding the secret information are. The smaller PSNR is, the greater the change of visual quality and the greater the image distortion after embedding the secret information are. PSNR is defined as

$$\text{PSNR} = 10 \times \log_{10} \left(\frac{(2^n - 1)^2}{\text{MSE}} \right). \quad (13)$$

SSIM evaluates labeled images by brightness, contrast, and structure. The structural similarity ranges from 0 to 1. When two images are the same, the value of SSIM is equal to 1. The higher the SSIM value is, the smaller the distortion of the algorithm is; the lower the SSIM value is, the greater the distortion of the algorithm is. The equation of SSIM is as follows:

$$\text{SSIM}(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}. \quad (14)$$

5.1. Analysis of Key Area Selection Results. The key area is the area containing important pathological features or diagnosis and treatment information, which is rich in texture and high in information content. This algorithm uses values to select key area. Table 1 shows the corresponding values of the six experimental images and whether the corresponding selected area is a disease sign area. It can be seen from the table that the region with the largest selected value is generally the region of disease sign. It can provide security for medical images.

Figures 4(a)–4(c), respectively, represent the effect of selecting the minimum value $P1$, the mean value $P3$, and the maximum value $P2$, and the QR code area is the key area selected. As can be seen from the figure, when the minimum value $P1$ is selected, the key area is the background area,

which does not have any disease warning information. When the mean value $P3$ is selected, the key area is an image block with low texture degree, which contains a small amount of information, but the information content is not rich and the security is not high. The best selection scheme is to select the scheme with the maximum value of $P3$. In Figure 4(c), the QR code occupies a large area of the lesion and has high safety.

5.2. Analysis of the Selection Result of Block Scheme. Block way is to have a certain influence on the embedded image visual quality. This study selected texture area of embedded computing MSE values as a standard of judging texture; too large blocks will reduce the accuracy of image calculation, which makes texture segmentation difficult to judge, but the smaller the image block, the higher the computational complexity. Therefore, the following comparison is made for the six images (a–f) according to different partitioning schemes to judge the best partitioning scheme.

In Figures 5 and 6, the abscissa represents the smallest block unit, and the ordinate is PSNR and SSIM, respectively. Among them, 8×8 means that the 512×512 image is divided into 4,096 small image blocks of 8×8 size without overlapping. The larger the partition, the smaller the values of SSIM and PSNR. As can be seen from Figure 5, PSNR decreased slowly before 64×64 partitioning and fluctuated greatly after 64×64 partitioning. As can be seen from Figure 6, SSIM decreases gradually with the increase of the minimum partitioning unit. SSIM and PSNR values of 8×8 , 16×16 , and 32×32 partitioning schemes do not change much. In this experiment, in order to obtain low PSNR and a certain computational accuracy, 64×64 is the optimal partitioning scheme, which can not only get accurate texture region but also keep low time complexity.

5.3. Smooth Region and Texture Region Embedding Results Analysis. For medical images, the texture region contains more information than the smooth region. With the help of the distortion caused by data embedding, the original content of the medical image can be protected to a certain extent, and the PSNR of the image can be controlled above 36, which does not cause the vigilance of the human visual system and realizes the protection of the image content, so as to improve the security of the algorithm.

In this study, six medical images are embedded into texture region and smooth region, respectively.

Figures 7 and 8 show the PSNR and SSIM values generated by embedding the image into the smooth region, the middle region, and the complex region, respectively. In Figure 7, the abscissa and ordinate PSNR of the image texture are provided to the texture of different degrees in Figure 8. The abscissa and ordinate SSIM of the image texture are provided according to the texture of different degrees. The high, medium, and low abscissa are embedded in the texture area, the middle area, and the smooth area, respectively. It can be seen that the PSNR values of each

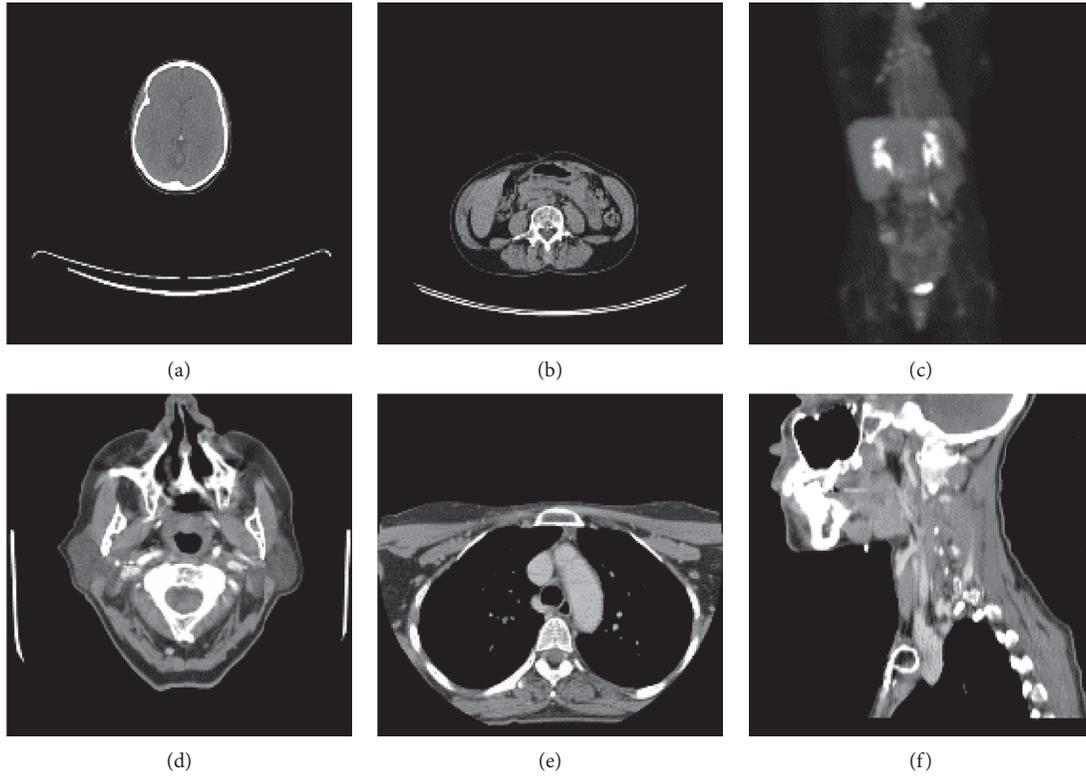


FIGURE 3: Experimental images. (a) Brain, (b) thorax, (c) spine, (d) encephalon, (e) lung, and (f) neck.

TABLE 1: Different CV value selection scheme.

	CV		
	$P1$	$P2$	$P3$
Brain	0	83.3684	24.8596
Thorax	0	67.8434	18.5000
Spine	0	60.9531	19.5786
Encephalon	0	77.8070	47.7426
Lung	0	88.6376	49.7015
Neck	0	107.7644	58.0105
Security	No	Yes	No

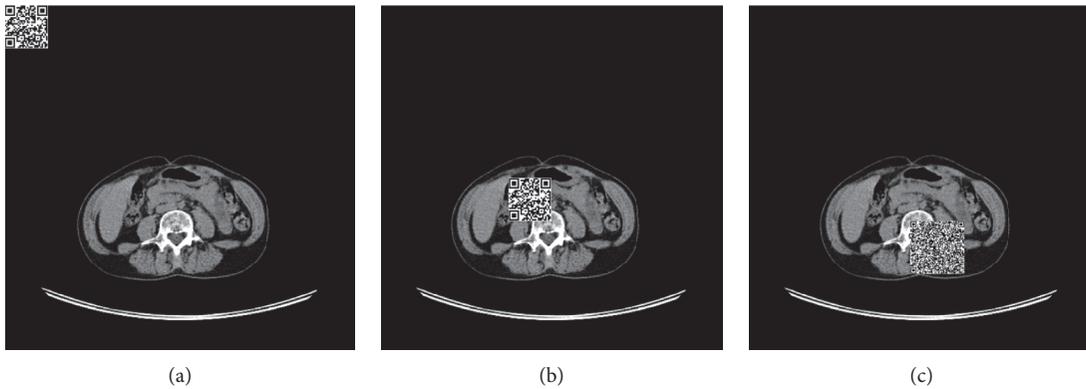


FIGURE 4: Different embedded CV value. (a) Minimum value, (b) mean value, and (c) maximum value.

regional selection scheme are maintained at 40–45 dB, but the smooth region does not contain any image information, so the high-texture region is selected as the key region. While

protecting the key region, certain distortion caused by embedding can also protect the information of the embedded region and further improve the image security.

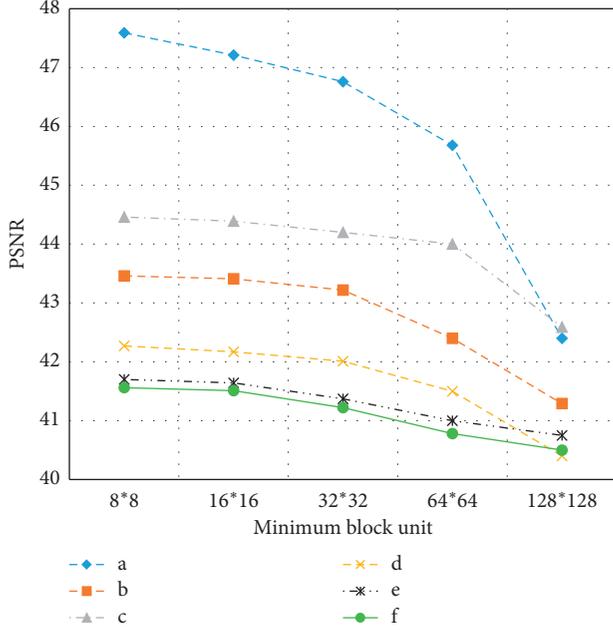


FIGURE 5: Block experiment PSNR comparison.

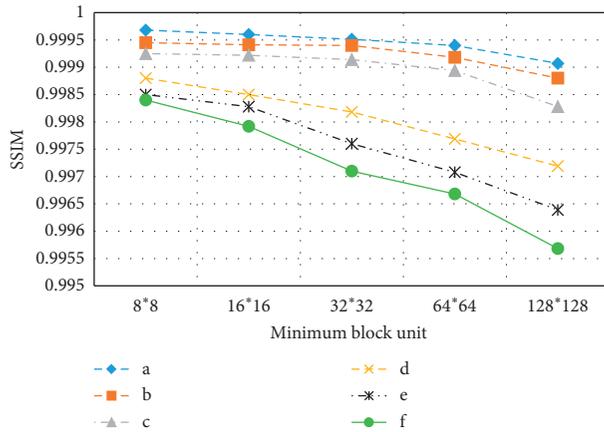


FIGURE 6: Block experiment SSIM comparison.

Because the sorting scheme is used in this paper, the experimental scheme shows better performance. The image blocks are sorted by texture degree, and the image blocks with complex texture are prioritized to improve the security of the algorithm. Table 2 shows the experimental results obtained by embedding high-textured regions under the 64×64 partitioning scheme, and T is the corresponding threshold value of each medical image dividing the textured regions. In practical application, different thresholds can be selected according to the size of secret information.

Figure 9 shows 6 medical images after the embedded watermark, firstly, the big image block as the areas that generate information secret information, generate QR code replacement key areas, the replacement after the image is divided into 64×64 subblock, use MSE values to select high-texture area of the image as an embedded area, and use the

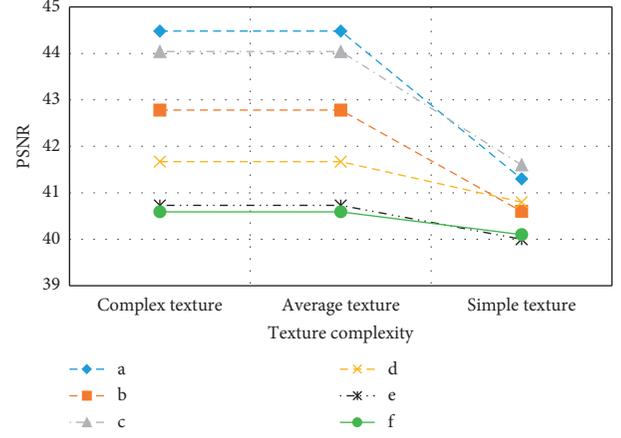


FIGURE 7: PSNR comparison.

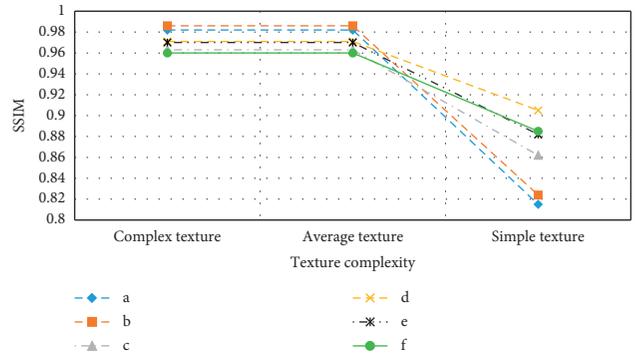


FIGURE 8: SSIM comparison.

TABLE 2: Test result.

Images	The size of the key area	Payload	Threshold	PSNR (dB)	SSIM
a	80×80	51200	5	44.48	0.982
b	80×80	51200	5	42.78	0.986
c	128×128	131072	10	44.04	0.963
d	128×128	131072	10	41.67	0.971
e	128×128	131072	10	40.73	0.970
f	128×128	131072	10	40.59	0.960

mean square error and histogram shifting technology to embed secret information.

Table 3 shows the performance comparison of the two embedding capacity methods proposed in [25, 26]. The data texture block based on CDMA algorithm in [25] is embedded into the selected detail subband because the pre-processing sequence is orthogonal embedded data, and the secret information is embedded into the cover image. The repeat spread spectrum sequence offsets most of the elements, so that the proposed large data embedding capacity can achieve higher visual quality. Reference [26] calculates the entropy of the image block to find the smooth block embedded in the watermark. The smoothed region is selected for embedding to obtain higher PSNR.

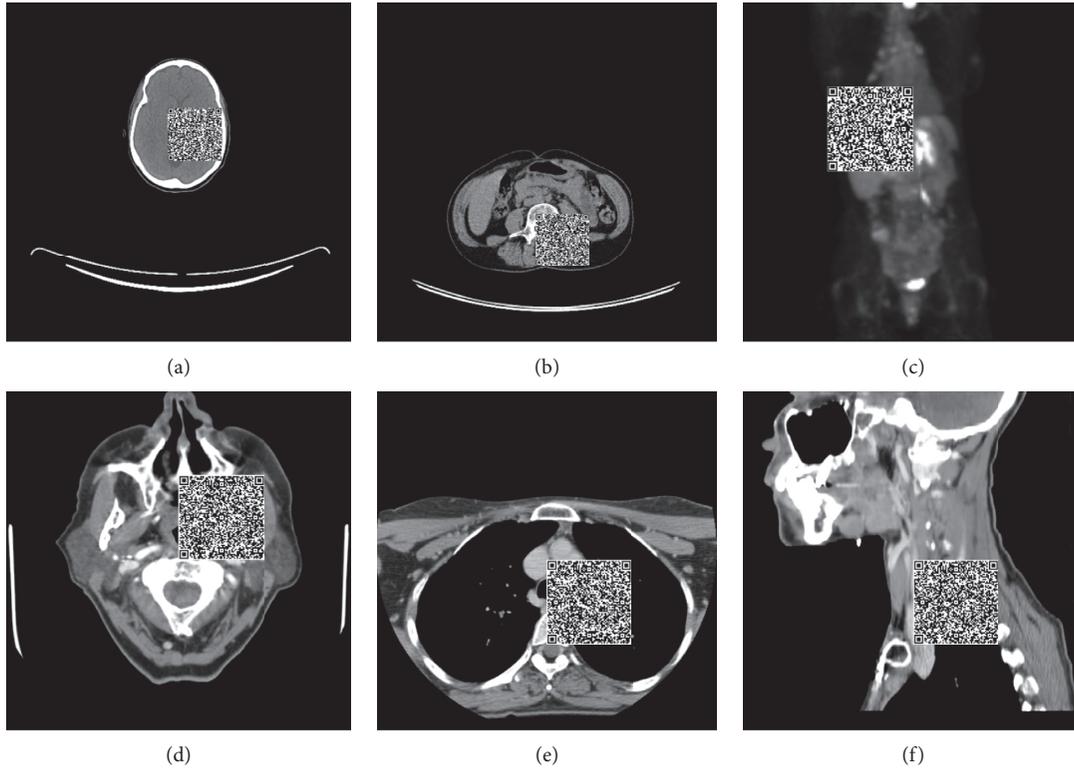


FIGURE 9: Medical image after embedding watermark. (a) Brain. (b) Thorax. (c) Spine. (d) Encephalon. (e) Lung. (f) Neck.

TABLE 3: Performance comparison.

Images		BPP	PSNR (dB)	SSIM
a	Proposed	0.195	44.48	0.982
	[25]	0.200	51.30	0.983
	[26]	0.350	56.43	N/A
b	Proposed	0.195	42.78	0.986
	[25]	0.352	51.24	0.998
	[26]	0.420	55.05	N/A
c	Proposed	0.500	44.04	0.963
	[25]	0.350	52.50	0.982
	[26]	0.400	55.71	N/A
d	Proposed	0.500	41.67	0.971
	[25]	0.350	52.12	N/A
	[26]	0.470	50.12	N/A
e	Proposed	0.500	40.73	0.970
	[25]	0.350	51.24	N/A
	[26]	0.320	56.90	N/A
f	Proposed	0.500	40.59	0.960
	[25]	N/A	N/A	N/A
	[26]	0.490	51.05	N/A

The purpose of this paper is to improve the content security of the image and control the PSNR of the embedded image above 36 dB to ensure that it is not detected by the human visual system. It can be seen from Table 3 that the PSNR of this algorithm is lower than that of traditional reversible

information hiding of medical images, but the PSNR value of each type of image is basically maintained at more than 36 dB. The experimental results show that the algorithm can achieve high image quality, and the receiver can recover the original medical image losslessly to avoid diagnostic bias.

6. Conclusion

In view of the high demand for medical image to the image content and the increasingly serious network security problems, this paper puts forward a reversible based information hiding algorithm of medical image key area protection. The key area is embedded as secret information to protect the image content; the generated QR code realizes the protection of image copyright and patient information and improves the security of image copyright. Compared with other medical image protection algorithms based on reversible data hiding, this algorithm uses QR code to improve the efficiency of image retrieval, uses information hiding to hide the existence of the patient area, controls the PSNR of the image above 40 dB, improves the imperceptibility of the lesion area, and realizes the security protection of medical image and the safe transmission of patient sensitive information. At the same time, only authorized customers can obtain the original image after embedding information and obtain the original fidelity medical image, so as to realize the security protection of medical image and the safe transmission of patient sensitive information in the open network environment. At the same time, with the help of QR code embedding, the scheme can also realize the safe retrieval of medical images and ensure the security of medical information. Experimental results show that this method is feasible and has a broad application prospect in the field of medical image information protection.

Future work will include larger-scale testing, including the computational costs. Additionally, we will explore cases where multiple regions are considered sensitive. Finally, we also plan to study the attack behavior. It can be imagined that malicious intrusion may try to change the QR code and texture area. Therefore, the appropriate strategy will need to identify the changes caused by the attack.

Data Availability

The software code and data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this study.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61802212 and 61872203), the Shandong Provincial Natural Science Foundation (ZR2019BF017 and ZR2020MF054), Major Scientific and Technological Innovation Projects of Shandong Province (2019JZZY010127, 2019JZZY010132, and 2019JZZY010201), Plan of Youth Innovation Team Development of Colleges and Universities in Shandong Province (SD2019-161), Jinan City "20 Universities" Funding Projects Introducing Innovation Team Program (2019GXRC031), and the Project of

Shandong Province Higher Educational Science and Technology Program (J18KA331).

References

- [1] Y. Xiang, D. Xiao, R. Zhang, J. Liang, and R. Liu, "Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer," *Information Sciences*, vol. 545, 2020.
- [2] D. Xiao, J. Liang, Q. Ma, Y. Xiang, and Y. Zhang, "High capacity data hiding in encrypted image based on compressive sensing for nonequivalent resources," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 1–13, 2019.
- [3] Z. Tang, S. Xu, H. Yao, C. Qin, and X. Zhang, "Reversible data hiding with differential compression in encrypted image," *Multimedia Tools and Applications*, vol. 78, 2018.
- [4] J. M. Barton, "Method and apparatus for embedding authentication information within digital data," US Patent US6512837B1, 2003.
- [5] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.
- [6] B. Ma and Y. Q. Shi, "A reversible data hiding scheme based on code division multiplexing," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 1914–1927, 2016.
- [7] R. Gurusamy and V. Subramaniam, "A machine learning approach for MRI brain tumor classification," *Computers, Materials, continua*, vol. 53, pp. 91–108, 2017.
- [8] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.
- [9] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.
- [10] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.
- [11] C. V. Kumar, V. Natarajan, and D. Bhogadi, "High capacity reversible data hiding based on histogram shifting for medical images," in *Proceedings of the 2013 International Conference on Communications & Signal Processing*, Melmaruvathur, India, April 2013.
- [12] M. H. Wu, J. Zhao, B. Chen, Y. Zhang, and J. Cheng, "Reversible data hiding based on medical image systems by means of histogram strategy," in *Proceedings of the 2013 3rd International Conference on Information Systems Engineering (ICISE)*, May 2013.
- [13] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption DWT-based algorithm for medical images," in *Proceedings of the 2017 14th International Conference on Computer Graphics, Imaging and Visualization (CGiV)*, IEEE Computer Society, Marrakesh, Morocco, May 2017.
- [14] M. Shalaby, M. T. Saleh, and H. N. Elmahdy, "Enhanced Arnold's cat map-aes encryption technique for medical images," in *Proceedings of the 2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, Giza, Egypt, October 2020.
- [15] J. Zhou, J. Li, and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," *IEEE Access*, vol. 8, 2020.
- [16] N. G. Pupa, "Cracking the "QR" code," *Journal of Property Management*, vol. 77, 2012.
- [17] V. Seenivasagam, R. Velumani, and M. M. I. Medicine, "A QR code based zero-watermarking scheme for authentication of

- medical images in teleradiology cloud,” *Computational and Mathematical Methods in Medicine*, vol. 2013, Article ID 516465, 16 pages, 2013.
- [18] J. Li, Z. Zhang, S. Li et al., “Reversible data hiding based key region protection method in medical images,” in *Proceedings of the 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pp. 1526–1530, San Diego, CA, USA, November 2019.
- [19] S. Weng, W. Tan, B. Ou, and J.-S. Pan, “Reversible data hiding method for multi-histogram point selection based on improved crisscross optimization algorithm,” *Information Sciences*, vol. 549, pp. 13–33, 2021.
- [20] K. Wang, G. Chen, Q. Ai, H. Cao, P. Zhou, and D. Wu, “Reversible data hiding based on structural similarity block selection,” *IEEE Access*, vol. 8, 2020.
- [21] X. Li, J. Li, B. Li, and B. Yang, “High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion,” *Signal Processing*, vol. 93, no. 1, pp. 198–205, 2013.
- [22] B. Ma, X. Wang, Q. Li et al., “Adaptive error prediction method based on multiple linear regression for reversible data hiding,” *Journal of Real-Time Image Processing*, vol. 16, no. 4, pp. 821–834, 2019.
- [23] H. Yao, F. Mao, Z. Tang, and C. Qin, “High-fidelity dual-image reversible data hiding via prediction-error shift,” *Signal Processing*, vol. 170, Article ID 107447, 2020.
- [24] J. M. Bardon, “Method and apparatus for embedding authentication information within digital data,” US Patent US5646997A, 2019.
- [25] B. Ma, B. Li, X. Y. Wang et al., “Code division multiplexing and machine learning based reversible data hiding scheme for medical image,” *Security and Communication Networks*, vol. 2019, Article ID 4732632, 9 pages, 2019.
- [26] S. Agrawal and M. Kumar, “Reversible data hiding for medical images using integer-to-integer wavelet transform,” in *Proceedings of the 2016 IEEE Students Conference on Electrical, Electronics & Computer Science*, March 2016.