Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 240749, 11 pages
http://dx.doi.org/10.1155/2014/240749

Research Article

A Novel Encryption Frame for Medical Image with Watermark Based on Hyperchaotic System

Shun Zhang, Tiegang Gao, and Lin Gao

College of Software, Nankai University, Wei Jin Road No. 94, Nankai District, Tianjin 300071, China

Correspondence should be addressed to Shun Zhang; shentengvip@gmail.com

Received 5 January 2014; Accepted 19 March 2014; Published 9 April 2014

Academic Editor: Jui-Sheng Lin

An encryption frame of medical image with watermark based on hyperchaotic system is proposed in this paper. Medical information, such as the patients' private information, data needed for diagnosis, and information for authentication or protection of medical files, is embedded into the regions of interest (ROI) in medical images with a high capacity difference-histogram-based reversible data-hiding scheme. After that, the watermarked medical images are encrypted with hyperchaotic systems. In the receiving end, the receiver with encryption key can decrypt the image to get similar images for diagnosis. If the receiver has the key for data hiding at the same time, he/she can extract the embedded private information and reversibly recover the original medical image. Experiments and analyses demonstrate that high embedding capacity and low distortion have been achieved in the process of data hiding, and, at the same time, high security has been acquired in the encryption phase.

1. Introduction

The rapid development of the Internet makes life more convenient than ever before. However, just as the old saying: every leaf has two sides, the Internet brings us not only convenience but also many problems. Leakage of privacy is one of the most important things. For example, medical information, such as EHRs (Electronic Health Records) [1], is often closely related to patients' privacies which should be kept secret. Medical images for diagnosis need to be protected in order to prevent malicious tampering. There are two ways for solving these problems: one is encryption, and the other one is information hiding. As a traditional solution of secure communication on insecure channels, encryption has been widely explored [2–10], and many of the encryption schemes have introduced chaotic systems to enhance the security of encryption. Information hiding (or data hiding) is a newly proposed way for secure communication although the ideology occurred quite a long time ago. With the development of data hiding and digital watermarking, many schemes have been proposed to embed information into medical images [1, 3, 11, 12] for the protection of private information and the authentication of medical images. These schemes utilized in medical images made full use of the intrinsic features of medical images and achieved nice results too. Obviously, both encryption and data hiding have their advantages in secure communication; what if we combine them together for better protection of medical image and private information?

Recently, some novel schemes combining the data hiding and encryption have been proposed [1, 3, 8, 12–16]. Among them, schemes can be divided into three categories: the first one is encryption before data hiding [13–16]; the second one is encryption after data hiding; the third one is fusion of encryption and data hiding [3]. From the information hider's point of view, information can be hidden in the spatial domain, the encrypted domain [13–16], or both of the two domains [8]. In [3], additional information is firstly coded with a quantization index modulation (QIM) method; then this coded information is encrypted with traditional encryption methods (such as RC4 algorithm); finally, the encrypted coded information is embedded into medical image with the simple least significant bit (LSB) substitution method. The scheme is not reversible due to the LSB substitution. Reversible data hiding schemes in encrypted images are proposed in [13, 14]. The image is encrypted with a stream

cipher, and then information is embedded into the encrypted images by modifying a small proportion of those encrypted data. In the receiving end, the encrypted image containing additional data is firstly decrypted to get similar versions of the original images; then, the embedded data can be extracted and the original image can be reversibly recovered with the data hiding key and the spatial correlation features in natural images [13]. It is reversible; however, the hiding capacity is rather low. In [14], an improvement is proposed to increase the hiding capacity of the scheme proposed in [13]. However, the hiding capacity is still not large enough after the improvement. The separation of data extraction and recovery of original images is achieved in [16]. There are two keys in the whole scheme. The image is firstly encrypted with the encryption key. Then, the encrypted image is passed to data hider. Additional information is embedded into the encrypted image with a data-hiding key. In the receiving end, the additional information can be extracted with only the data-hiding key. The similar (not reversible) image can be recovered with only the encryption key. If someone has the two keys, he/she can both extract the additional information and reversibly recover the original image. In [15], medical images are firstly divided into blocks; then, three LSB planes substitution is utilized in the regions of noninterest (RONI) in medical images for hiding the additional data. In [8], a reversible data hiding scheme in encrypted images by reserving room before encryption is proposed. The self-embedding of LSB planes guarantees the reversibility of LSB substitution embedding.

Different from all the schemes mentioned above, a novel encryption frame for medical image with watermark based on hyperchaotic system is proposed in this paper. Additional data, such as patients' private information and data for the authentication of medical images, is firstly embedded into the ROI of the original medical image with a difference-histogram shifting method. Then, the medical image with data embedded is encrypted with a hyperchaotic system. After that, the encrypted medical images with watermarks can be transmitted publicly and safely on the Internet. Besides, if there are not clear distributions of ROI and RONI in some images, the proposed scheme can still be imposed on the whole images. In the receiving end, the encrypted image is firstly decrypted to get the similar image with watermark. Then, the ROI of the image with hidden data is detected and hidden data is extracted. Finally, the original medical image is reversibly recovered. Different from most existing data hiding methods in medical images that hide data in the RONI of medical images, the proposed scheme hides data in the ROI of medical images. Moreover, histograms of difference image blocks are utilized for better increasing the hiding capacity and decreasing the distortion of reversible data-hiding scheme. The hyperchaotic system can produce large key space and sensitivity for encryption and this guarantees the safety of the communication.

2. Related Works

2.1. The Hyperchaotic System for Encryption. Chaotic system is a kind of nonlinear system that is very sensitive to the initial states and system parameters. The nonperiodic features and pseudorandomness of chaotic systems are beneficial to encryption. Encryption scheme based on chaos was proposed in 1989 [17]. Since then, many encryption schemes based on different chaotic systems have been proposed in the following. For example, an encryption scheme based on logistic map was proposed in [18]. In [2], Arnold cat map was introduced to shuffle the positions of image pixels, and a hyperchaotic system was utilized to confuse both the plain-image and the cipher-image. In [19], an image encryption scheme based on a three dimensional (3D) chaotic map, which could defeat many existing attacks, was proposed. Hyperchaotic system has more than one positive Lyapunov exponent; thus, the complexity of encryption schemes based on hyperchaotic system is higher; therefore, it is more suitable for the design of encryption schemes.

2.2. Reversible Data Hiding. Reversible data hiding refers to the process to hide data into cover media, which guarantees the reversible recovery of the original cover image after data extraction. There are three main categories of reversible data-hiding schemes; the first one is compression based [20], the second one is difference expansion based [21], and the third one is histogram modification based [22]. Schemes based on histogram modification cause less distortion to the cover image, so they are suitable for data hiding in images that require higher qualities, such as medical images. However, the obvious drawback of histogram modification-based data-hiding schemes is that the hiding capacity is limited. In order to increase hiding capacity of this kind of schemes, some measures such as raising the peak points' height of the histogram or increasing the number of peak points can be utilized. In [23], an optimization of the prediction accuracy of the target pixels was proposed to raise the heights of the peak points in the histogram to increase the embedding capacity. A (k, n)-image reversible hiding method that can restore the cover image and k confidential images from n stego-image was proposed to increase the security of the data hiding [24]. In [25], the embedding capacity was increased by multi-employing invariability of the mean value of $(n-1)$ pixels, and the embedding distortion is greatly controlled by embedding more bits into smooth image blocks and fewer bits into the other blocks with complex texture. In [26], a multilevel embedding scheme was proposed to increase the capacity of histogram modification-based reversible data scheme. In [27], the original image was firstly sampled and then a predicted image based on sampled images was acquired. The difference images between the predicted image and these sampled images were calculated to get the histogram of difference image for data embedding.

2.3. ROI Detection of Medical Images. Different from natural images, medical images always have consecutive region of interest (core content that contains clinical findings) and region of noninterest (background), denoted by ROI and RONI for short, respectively. Many selection algorithms have been proposed to separate the ROI and RONI. Some early but still-in-use methods, such as [12], regard the ROI as a rectangle. These methods are easy and flexible but not

intelligent. Recently, some new methods have been proposed [1, 11]. In [11], a pixel-based scanning method from both (left and right) sides to the center was proposed, and a threshold determined the contour of ROI. The average intensity of the RONI blocks should approach to zero, while the average intensity of the ROI blocks would be much bigger. Therefore, a block-based scheme was used to calculate the average intensity in [1]. In order to get better performance, a filter was used to preprocess the images before energy calculation.

Most of the existing watermarking schemes embed information into RONI because they cause no distortion to the core area of medical images. However, these RONI embedding schemes may cause significant changes to cover images if the ROI and RONI are considered as a whole. The RONI embedding is easily detected by others. Besides, the RONI is usually cropped when preprocessing medical images for better storage. It is inconvenient and insecure to embed data in the RONI.

3. Proposed Encryption Scheme of Medical Image with Watermark

The flowchart of the whole scheme is presented in Figure 1. Firstly, a block-energy-based algorithm is proposed to determine the ROI of the original medical image. Secondly, the preprocessed additional data is embedded into the ROI of the medical image with a histogram modification-based data-hiding scheme. Finally, the watermarked image is encrypted utilizing a hyperchaotic system. The decryption and data extraction process are presented in Figure 2. After receiving the encrypted medical image, the receiver decrypts it to get medical image with watermarks. Then, ROI of the watermarked image is detected. Finally, additional data is extracted and the original image is recovered reversibly.

3.1. ROI Detection. The medical image with size $N_1 \times N_2$ is firstly divided into blocks with size $n_1 \times n_2$. Obviously, the amount of blocks is $(N_1 \times N_2)/(n_1 \times n_2)$. Then, the average energy of every block is calculated by the following:

$$\text{ave\_energy}(m,n) = \frac{\left(\sum_{i=1}^{n_1}\sum_{j=1}^{n_2} I(i,j)^2\right)}{(n_1 \times n_2)}, \quad (1)$$

where $\text{ave\_energy}(m,n)$ represents the average energy of the current block, (m,n) represents the position of image blocks, and $I(i,j)$ is pixel value. Finally, compare the average energy value of every block with an adaptive threshold T to determine whether a block belongs to ROI or not: if $\text{ave\_energy}(m,n) > T$, then it belongs to the ROI; else, the block belongs to the RONI.

3.2. Reversible Data Hiding Based on Histogram Modification. Additional information is preprocessed and encoded into binary stream before it is embedded into ROI blocks of medical images. A reversible data-hiding algorithm based on histogram of difference image blocks is proposed for the information embedding. This algorithm can be preceded together with ROI detection process. Once one ROI block is detected, it can be used for information embedding immediately. The detailed algorithm is described as follows.

(1) Preprocess and encode additional data into binary streams and divide the binary streams into segments according to ROI blocks.

(2) Scan every ROI block pixel by pixel to get the pixel sequence $\text{se}(m,n)$, where (m,n) represents the position of image blocks.

(3) Calculate difference of neighbor pixels of $\text{se}(m,n)$ to get difference sequence $\text{sed}(m,n)$.

(4) Construct histogram of difference sequence $\text{sed}(m,n)$, and then find two peak points p_1 and p_2 and their corresponding nearest zero points z_1 and z_2.

(5) Shift the histogram bidirectionally and embed bit streams of medical information into the gaps, and then difference pixel sequence with hidden information is acquired, denoted by $\text{sede}(m,n)$.

(6) Form the pixel sequence of watermarked blocks $\text{seem}(m,n)$ with the original pixel sequence $\text{se}(m,n)$ and $\text{sede}(m,n)$. For every element $\text{seem}(m,n,i)$ in the block sequence $\text{seem}(m,n)$: $\text{seem}(m,n,i) = \text{se}(m,n,i-1) + \text{sede}(m,n,i)$, where $\text{se}(m,n,i-1)$ and $\text{sede}(m,n,i)$ are elements of pixel sequence $\text{se}(m,n)$ and $\text{sede}(m,n)$, respectively.

(7) Reconstruct the block with sequence $\text{seem}(m,n)$.

(8) Repeat step (2) to step (7) until all the information is embedded into different blocks of ROI.

The threshold T for the detection of ROI of medical images and the sizes of ROI blocks and additional information are encoded as the key for data extraction. The data extraction key can be sent to the receiving end alone or along with the watermarked medical image. It can be encrypted by symmetric encryption algorithm or by the public-key encryption algorithm. In the symmetric encryption scheme, the key for data extraction is encrypted with the same key that is shared between the sending end and the receiving end. In public-key encryption, the data extraction key is encrypted by the public key in the sending end, whereas it can be decrypted by the private key of the receiver. It is more secure to use the public-key encryption for the delivery of key for data extraction.

3.3. Encryption Scheme Based on Hyperchaotic System. The medical image with watermark is encrypted with a series of random numbers. A hyperchaotic system by Gao et al. [28] is used to generate the discrete random numbers for encryption:

$$\begin{aligned} \dot{y}_1 &= a(-y_1 + y_2), \\ \dot{y}_2 &= dy_1 + cy_2 - y_1 y_3 - y_4, \\ \dot{y}_3 &= y_1 y_2 - by_3, \\ \dot{y}_4 &= y_1 + k, \end{aligned} \quad (2)$$

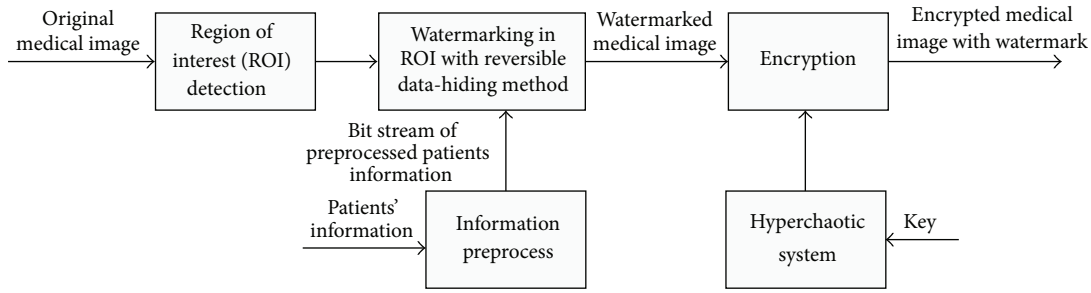


Figure 1: Block diagram of information embedding and encryption.

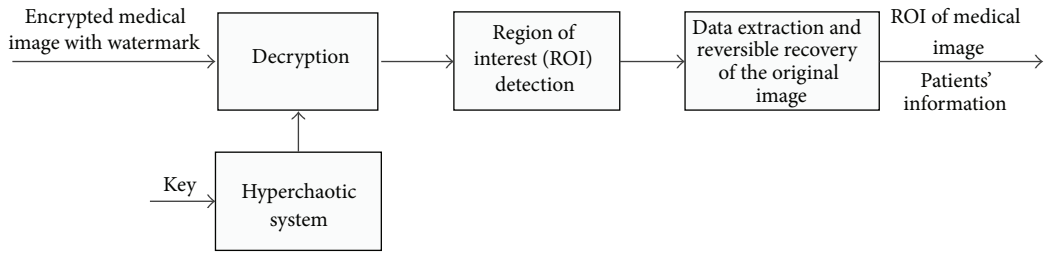


Figure 2: Block diagram of decryption and information extraction.

where a, b, c, d, and k are parameters, and when $a = 36$, $b = 3$, $c = 28$, $d = -16$, and $-0.7 \le k \le 0.7$, the system is hyperchaotic. The attractors of the hyperchaotic system with parameters $a = 36$, $b = 3$, $c = 28$, $d = -16$, and $k = 0$ are shown in Figure 3.

Then, the encryption algorithm is as follows.

(1) Iterate the hyperchaotic system for N_0 times by Runge-Kutta algorithm to get the four discrete states sequences y_k $(k = 1, 2, 3, 4)$ of the system.

(2) Then, these decimal fractional sequences are preprocessed for encryption as follows:

$$x_k(i) = \mathrm{mod}\left(\left(\mathrm{abs}\left(y_k(i)\right) - \mathrm{floor}\left(\mathrm{abs}\left(y_k(i)\right)\right)\right) \times 10^{13}, 256\right), \quad (3)$$

where $x_k(i)$ is the ith value of sequence x_k, $\mathrm{abs}(x)$ represents the absolute value of x, and $\mathrm{floor}(x)$ returns the nearest integers less than or equal to x.

(3) Construct the encryption sequence $E(j)$ with x_k $(k = 1, 2, 3, 4)$:

$$E(j) = x_k(i), \quad (4)$$

where $k = j - (i-1) \times 4$, $i = \{1, 2, \ldots, N_1 \times N_2/4\}$, $j = \{1, 2, \ldots, N_1 \times N_2\}$, and $N_1 \times N_2$ is the size of image to be encrypted.

(4) Do exclusive OR (XOR) operation between every pixel $P(j)$ of the image to be encrypted and encryption sequence E:

$$C(j) = P(j) \oplus E(j), \quad (5)$$

where $C(j)$ represents the ciphered pixel and XOR means bitwise exclusive OR; then, $C = \{C_1, C_2, \ldots, C_{N_1 \times N_2}\}$ is written back to the encrypted image.

The initial value and iteration parameters of the hyperchaotic system are encoded as the key, denoted by k_1, for decryption.

3.4. Decryption Scheme and Data Extraction. The encrypted medical image with hidden information is received by the remote receiver for diagnosis. The original medical image is reversibly recovered and the information embedded is extracted with the following steps.

(1) Generate the encryption sequence E with key k_1 as the encryption process.

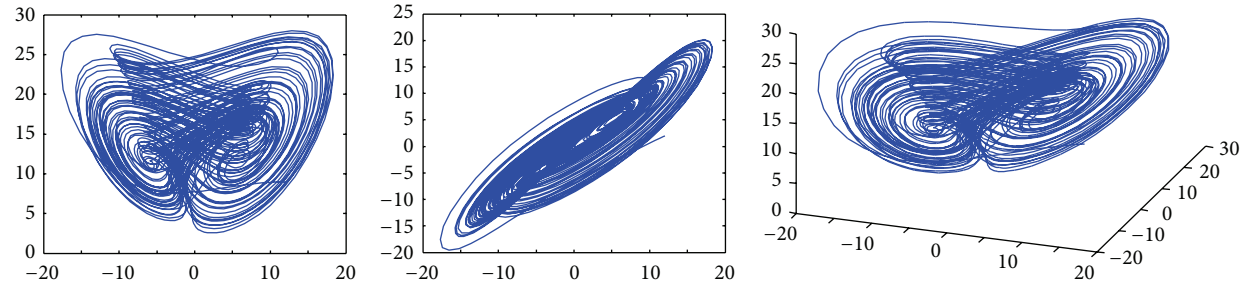
(2) Do XOR between the encrypted image C and the encryption sequence E:

$$P(j) = C(j) \oplus E(j), \quad (6)$$

where $P(j)$ represents the decrypted pixel and $P = \{P_1, P_2, \ldots, P_{N_1 \times N_2}\}$ is the decrypted image.

(3) Divide image P into blocks with the same sizes as that of embedding process, and then calculate the average energy of each block to determine the ROI of the image with threshold T, which is the same as the threshold T of the ROI detection procedure in Section 3.1.

(4) Calculate the differences of pixels in every ROI block to get difference pixel sequence $\mathrm{sede}(m, n)$. Then,



(a) y1-y3 bit plane (b) y1-y2 bit plane (c) 3D plot of y1-y2-y3 bit plane

Figure 3: Hyperchaotic attractors of system (2).

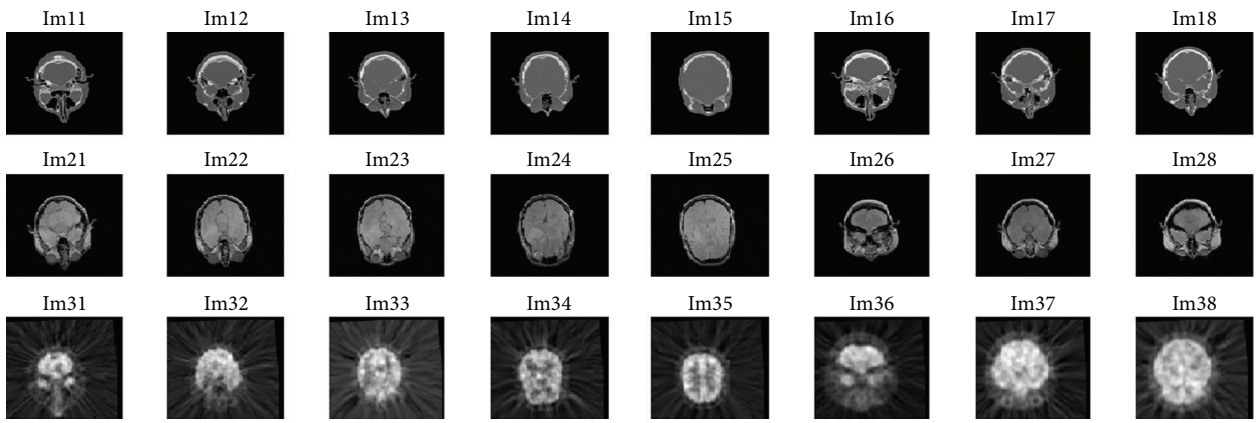


Figure 4: Medical images with different sizes.

scan the sequence sede (m, n) to extract the hidden information. Consider the following.

(a) If the two peak points $p_1 > p_2$, then the bit "0" is extracted when the pixel value p_1 or p_2 in the sequence sede (m, n) is encountered, and the bit "1" is extracted when the pixel value $p_1 + 1$ or $p_2 - 1$ in sequence sede (m, n) is encountered.

(b) Or else, the bit "0" is extracted when the pixel value p_1 or p_2 in sequence sede (m, n) is encountered, and the bit "1" is extracted when pixel value $p_2 + 1$ or $p_1 - 1$ in sequence sede (m, n) is encountered.

(5) Reversibly recover the original sequence se (m, n) of every ROI block through an iteration of sede (m, n), seem (m, n), and se (m, n) itself: sede (m, n, i) = seem (m, n, i) − se $(m, n, i - 1)$ and se (m, n, i) = se $(m, n, i - 1)$ + sed (m, n, i), where sed (m, n, i) is the elements of the sequence sede (m, n).

The reason why the thresholds in the receiving end are the same as the original one is that the embedding process-based histogram of difference image blocks causes little distortion to the original image, which can be ignored in the calculation of average energy of ROI blocks.

4. Experimental Results and Analysis

Three groups of test medical images with different sizes are presented in Figure 4. In Figure 4, the sizes of images for test are 512 × 512, 256 × 256, and 128 × 128 in the three rows, respectively.

4.1. ROI Detection. For the tested images with different sizes, such as 512 × 512, 256 × 256, and 128 × 128, different sizes of blocks and different thresholds are utilized. The block size is equal to 32 × 32 for images with size 512 × 512, and the threshold is $T = 9$; the block size is equal to 16 × 16 for images with size 256 × 256, and the threshold is $T = 1000$; the block size is equal to 8 × 8 for images with size 128 × 128, and the threshold is $T = 2000$. The test results are presented, respectively, in Figure 5. The regions marked white are used for information embedding. Different sizes and different shapes of ROI can be acquired with different parameters (block size and threshold) according to actual requirements. In Figure 5, subimages (a), (b), and (c) are the original medical images and their corresponding detected ROIs are subimages (d), (e), and (f).

4.2. Original Medical Image versus Image with Watermark. The original medical images and images after reversible data

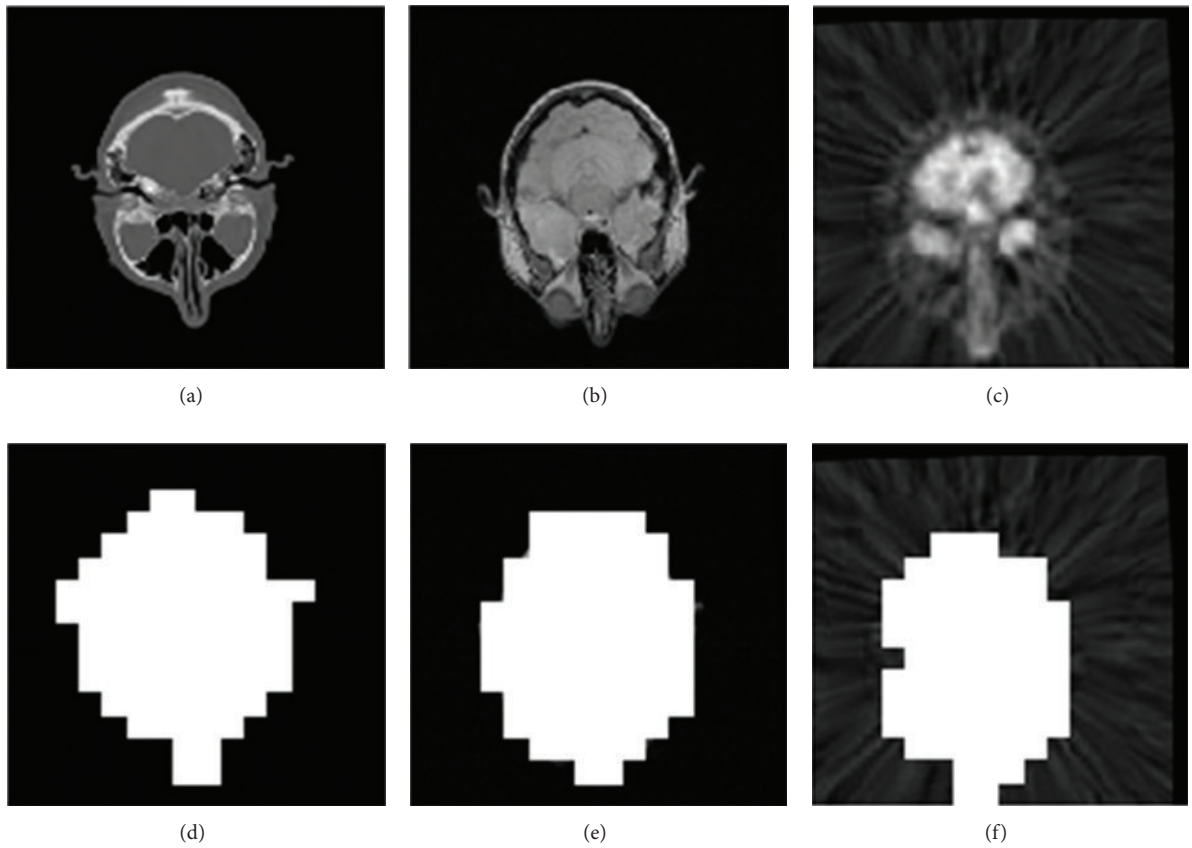


Figure 5: ROI detection of different images with different sizes.

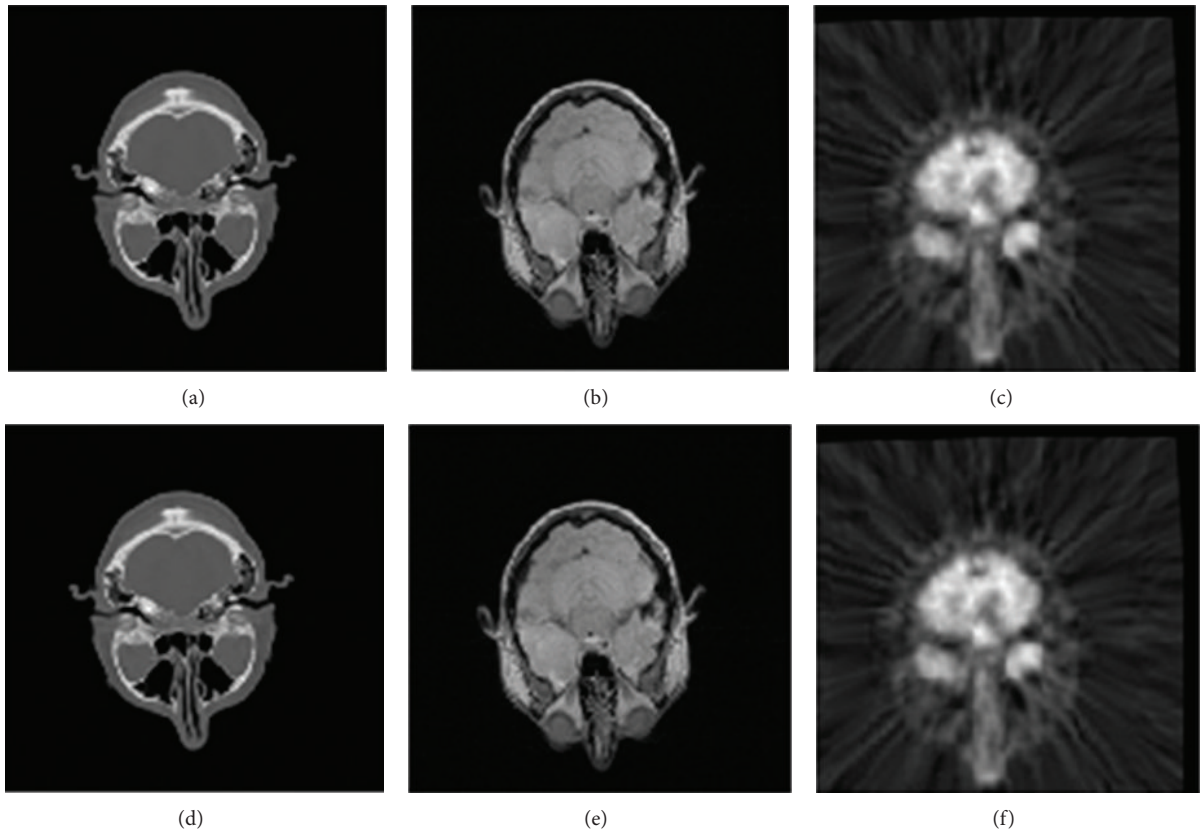
Table 1: Capacity and PSNR of medical images with size of 512 × 512 with block size of 32 × 32.

Images	Im11	Im12	Im13	Im14	Im15	Im16	Im17	Im18
Capacity (bit)	42617	42593	48997	52359	51644	41515	433448	49221
PSNR (dB)	56.24	56.04	55.70	56.01	56.08	55.72	56.05	55.58
ROI blocks number	86	83	85	85	82	87	87	88
Threshold	9	9	9	9	9	9	9	9

hiding are presented in Figure 6. In Figure 6, image (d) is the watermarked image of image (a), with 32 bits embedded into every 32 × 32 block, and the total number of ROI blocks is 86. The PSNR between image (a) and image (d) is 58.82. Image (e) is the watermarked image of image (b), with 16 bits embedded into every 16 × 16 block, and the total number of ROI blocks is 84. The PSNR between image (b) and image (e) is 57.85. Image (f) is the watermarked image of image (c), with 8 bits embedded into every 8 × 8 block, and the total number of ROI blocks is 74. The PSNR between image (c) and image (f) is 60.16.

4.3. Embedding Capacity and PSNR of Medical Images with Different Sizes. The embedding capacity and the corresponding PSNR of different medical images of different sizes are presented in Tables 1, 2, and 3. Medical images of different sizes are divided into different blocks; therefore, the numbers of ROI blocks are different due to the block energy-based ROI detection method. Besides, the thresholds for ROI detection of different medical images are different too. According to our experiments, the proper amount of blocks of every medical image is 256 (i.e., 16×16). Higher capacities with higher PSNR have been achieved compared with the scheme proposed in [16]. To ensure the reversibility, at least 32 × 32 pixels are needed for one bit information in [13], which means that at most 256 bits can be embedded into one image with size 512× 512, which is lower compared with the proposed scheme.

4.4. Encryption and Decryption. The experimental results of encryption and decryption are shown in Figures 7, 8, and 9. The watermarked medical images, their encrypted versions, their right decrypted versions, their wrong decrypted versions, and their corresponding histograms with sizes 512 × 512, 256 × 256, and 128 × 128 are presented in the three groups of figures, respectively. It can be clearly seen that without the correct key, the decrypted images are



(a) (b) (c)

(d) (e) (f)

Figure 6: Medical images and their corresponding watermarked images.

Table 2: Capacity and PSNR of medical images with size of 256 × 256 with block size of 16 × 16.

Images	Im21	Im22	Im23	Im24	Im25	Im26	Im27	Im28
Capacity (bit)	4073	3919	4000	4627	4360	3419	3819	3635
PSNR (dB)	56.78	56.88	56.97	56.65	56.87	56.61	57.58	57.68
ROI blocks number	93	89	89	89	89	74	75	76
Threshold	100	100	100	100	100	100	100	100

Table 3: Capacity and PSNR of medical images with size of 128 × 128 with block size of 8 × 8.

Images	Im31	Im32	Im33	Im34	Im35	Im36	Im37	Im38
Capacity (bit)	702	983	601	684	642	1147	1219	1851
PSNR (dB)	59.90	58.27	60.92	60.21	60.53	57.46	56.94	55.51
ROI blocks number	74	88	64	74	67	93	112	144
Threshold	2000	2000	5000	2000	2000	2000	2000	2000

random noise like pixels. In each group of images and their corresponding histograms, subimage (d) is the decrypted images with random streams. Subimage (e) is the decrypted images with wrong initial values, and only 10^{-10} difference is introduced in the chaotic system. Actually, the initial values of hyperchaotic system are $[12, 2, 9, 1]$ in the encryption while in the wrong decryption 2 the initial values are $[12, 2, 9, 1.0000000001]$. Therefore, high sensitivity has been achieved through the hyperchaotic system.

4.5. Security Analysis. Fine encryption methods should resist different kinds of attacks, such as known-plain-text, cipher-text-only attack, differential attack, statistical attack, and various brute-force attacks [12]. Different security analyses are performed in the following.

(a) Key Space Analysis. Key space should be large enough to make brute-force attacks infeasible. In the proposed scheme, 13-bit rational numbers are selected for the generation of

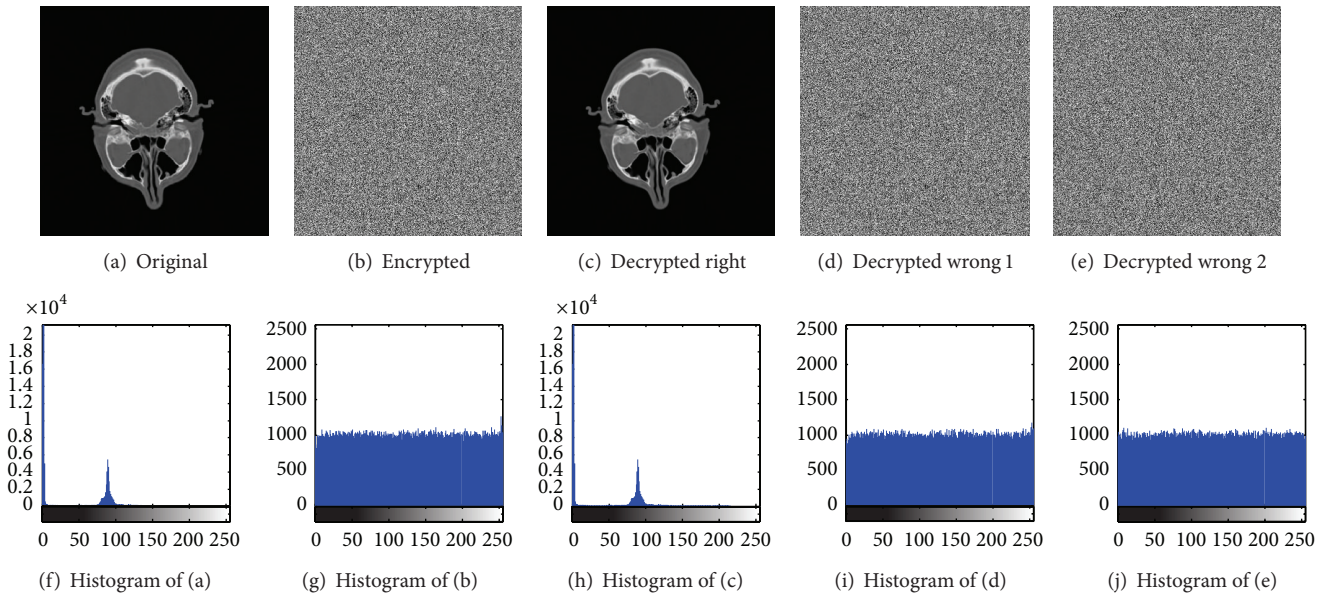


Figure 7: Encryption and decryption of medical image with size 512 × 512.

Table 4: Coefficients of images of different sizes.

Coefficients	Plain-image			Cypher-image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Im11	0.9935	0.9897	0.9847	0.0193	−0.0154	0.0032
Im21	0.9753	0.9711	0.9610	0.0124	0.0080	0.0445
Im31	0.9862	0.9849	0.9730	0.0177	−0.0081	−0.0325

random sequences, which are large enough to resist all kinds of brute-force attacks.

(b) Correlation of Two Adjacent Pixels. In this section, correlation between two adjacent pixels is calculated by the following formulas; 4096 pairs of two adjacent horizontal pixels, two adjacent vertical pixels, and two adjacent diagonal pixels are randomly selected, respectively. Consider the following:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2,$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} E\left(x - E(x)\left(y - E(y)\right)\right), \tag{7}$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}.$$

Figure 10 presents the correlation of im11 from Figure 4. The correlation of two adjacent pixels of the same row, of the same column, and of the same diagonal is presented, respectively. The correlation of the original image is presented in the first row, while correlation of the encrypted image is presented in the second row. The detail coefficients r_{xy} of im11, im21, and im31 from Figure 4 are presented in Table 4.

4.6. Special Features Compared with Existing Schemes

(a) Information Embedding into ROI of Medical Images. Existing watermarking or data-hiding schemes [1, 11, 12] for medical images embed information into RONI, which may cause no distortion to the ROI. However, these kinds of methods can only be applied in medical images with RONI, but usually there are large quantities of medical images that do not have RONI, and this may result in that the scheme is unable to be used. Another advantage of ROI embedding schemes is that little distortion will be caused to the image, which means that information hiding is imperceptible. Due to the embedding scheme based on histogram modification, the ROI detection process of information extraction and original image recovery can use the same threshold used in the information embedding process.

(b) Reversible Data Hiding with High Capacity and High PSNR. In the proposed reversible data-hiding scheme, histograms of difference image blocks are used. For medical images, distortion must be low after data hiding. The histogram-based schemes change the grey value of every

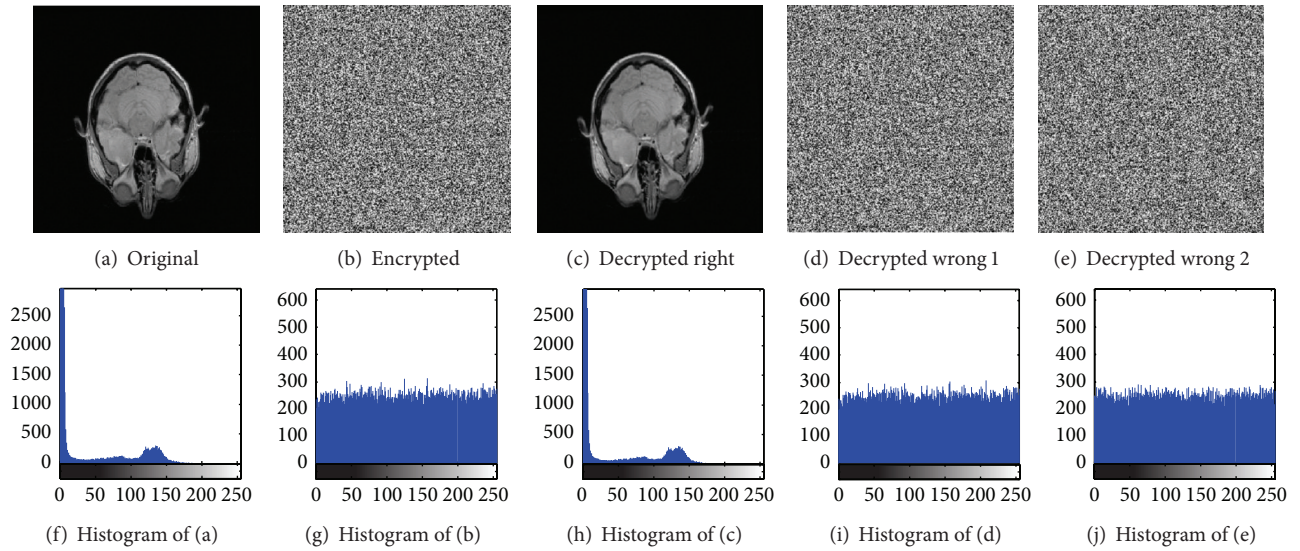


Figure 8: Encryption and decryption of medical image with size 256 × 256.

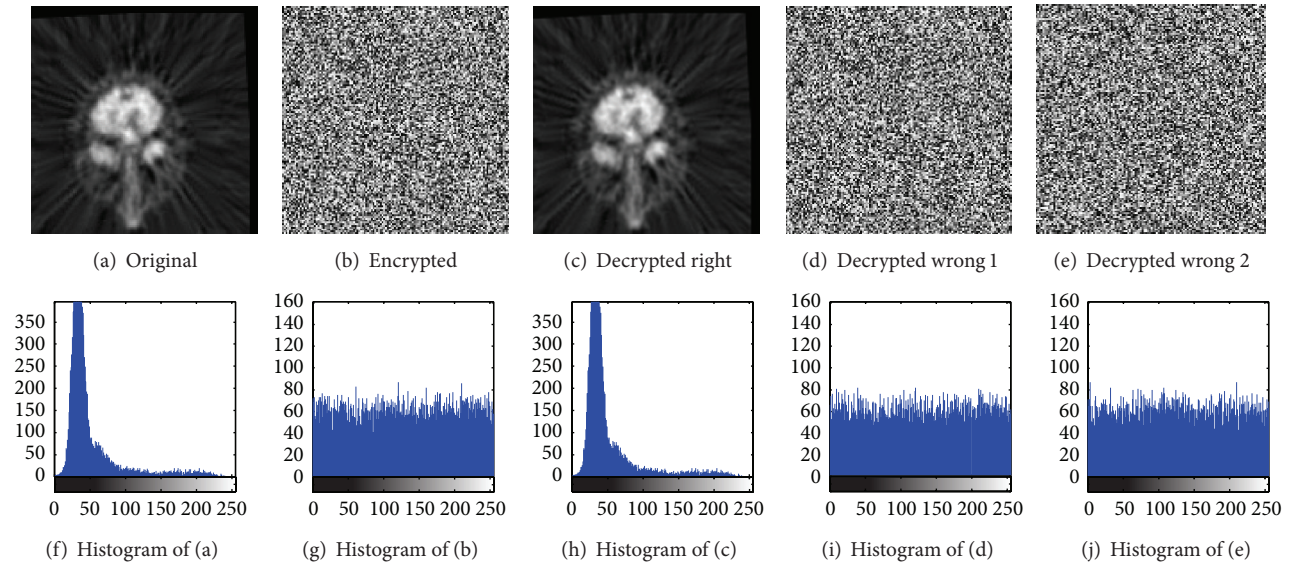


Figure 9: Encryption and decryption of medical image with size 128 × 128.

pixel by one at most (increasing by one, decreasing by one, or remaining the same), which guarantees the high PSNR between the original image and its watermarked image. Besides, the height of peak point of histogram and number of peak-zero point pairs are both increased through a reasonable pixel-by-pixel scan pattern and the block-divide operation; thus, high capacity is achieved in the scheme. Thus, compared with [13, 14, 16], higher capacity and higher image quality are achieved after reversible data hiding. Scheme proposed in [3] can achieve high capacity; however, it is not reversible.

(c) Combination of Chaos-Based Encryption and Information Hiding. There are many schemes designed for privacy protection of medical images and their corresponding EHRs, most of which can be catalogued into two aspects: encryption and information hiding. Encryption schemes are extensively used in information communication and image transfer on public channels. In the proposed scheme, without the correct key, random like pixels will never be decrypted; even with a very small error, an entire different image will be decrypted. However, encrypted images' transfer on the Internet may arouse other people's attention, and the intruder may be stimulated to decrypt it. Thus, just encryption always makes it insecure for information transmission in some degree. Reversible data-hiding scheme can conceal the communication process of hidden information and thus has its inherent advantage in secure communication. The combination of encryption and information hiding offers a multilevel protection of

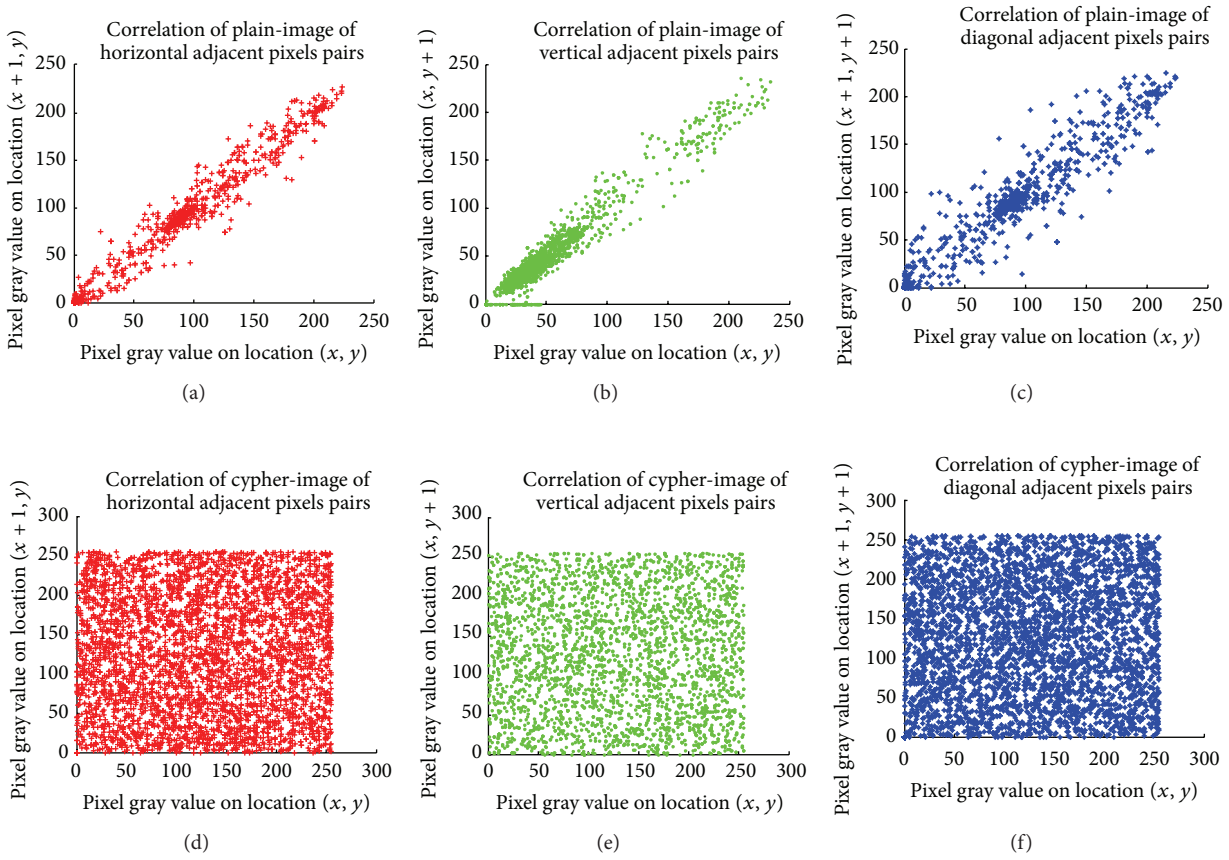


Figure 10: Correlations of two adjacent pixels in the plain-image and in the cipher-image of im11.

information communication. Besides, different from existing joint encryption and data-hiding schemes [3, 8, 13–16], the reversible data-hiding process is done before encryption.

4.7. Applications Based on the Proposed Scheme. The hidden data in the proposed scheme can be any digitalized information. Besides patients' EHRs mentioned above, the information for authentication and protection of medical images can also be embedded with the proposed scheme. Thus, various kinds of applications can be implemented.

5. Conclusions

An encryption scheme frame for medical image with watermarking is proposed in this paper. Private medical information is embedded into ROI of medical images with a histogram-based reversible data-hiding scheme. The watermarked medical image is encrypted with a hyperchaotic system. In the receiver end, medical information can be extracted and the original medical image can be reversibly recovered. Compared with standalone encryption or watermarking scheme, the proposed scheme is a fusion of encryption and watermark, and it not only has large space of secret key, but it also has large capacity of watermark embedding. Experimental results testified the effectiveness of the scheme.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to thank the support from National Science Fund of China (Grant no. 60873117) and Key Program of Natural Science Fund of Tianjin (Grant no. 11JCZDJC16000), China.

References

[1] V. Fotopoulos, M. L. Stavrinou, and A. N. Skodras, "Medical image authentication and self-correction through an adaptive reversible watermarking technique," in *Proceedings of the 8th IEEE International Conference on BioInformatics and BioEngineering (BIBE '08)*, pp. 1–5, October 2008.

[2] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[3] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 891–899, 2012.

[4] M. François, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.

[5] Z. Wei, Y. Wu, X. Ding, and R. H. Deng, "A scalable and format-compliant encryption scheme for H. 264/SVC bitstreams," *Signal Processing: Image Communication*, vol. 27, pp. 1011–1024, 2012.

[6] M. Ghebleh, A. Kanso, and H. Noura, "An image encryption scheme based on irregularly decimated chaotic maps," *Signal Processing: Image Communication*, 2013.

[7] J. B. Lima, E. A. O. Lima, and F. Madeiro, "Image encryption based on the finite field cosine transform," *Signal Processing: Image Communication*, vol. 28, pp. 1537–1547, 2013.

[8] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[9] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Processing: Image Communication*, vol. 28, pp. 292–300, 2013.

[10] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Processing: Image Communication*, vol. 28, pp. 670–680, 2013.

[11] V. Fotopoulos, M. L. Stavrinou, and A. N. Skodras, "Authentication and self-correction in sequential MRI slices," *Journal of Digital Imaging*, vol. 24, no. 5, pp. 943–948, 2011.

[12] F. Rahimi and H. Rabbani, "A dual adaptive watermarking scheme in contourlet domain for DICOM images," *BioMedical Engineering Online*, vol. 10, article 53, 2011.

[13] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[14] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[15] A. Lavanya and V. Natarajan, "Watermarking patient data in encrypted medical images," *Sadhana-Academy Proceedings in Engineering Sciences*, vol. 37, pp. 723–729, 2012.

[16] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[17] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[18] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238–242, 2002.

[19] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[20] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Electronic Imaging*, vol. 2002, pp. 572–583, 2002.

[21] 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.

[22] 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. 354–361, 2006.

[23] S. L. Lin, C. F. Huang, M. H. Liou, and C. Y. Chen, "Improving histogram-based reversible information hiding by an optimal weight-based pre-diction scheme," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, pp. 19–33, 2013.

[24] H. Gwoboa, H. Ying-Hsuan, C. Chin-Chen, and L. Yanjun, "(k, n)-image reversible data hiding," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, pp. 152–164, 2014.

[25] S. Weng, S. C. Chu, N. Cai, and R. Zhan, "Invariability of mean value based reversible watermarking," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, pp. 90–98, 2013.

[26] C.-C. Lin, W.-L. Tai, and C.-C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recognition*, vol. 41, no. 12, pp. 3582–3591, 2008.

[27] K.-S. Kim, M.-J. Lee, H.-Y. Lee, and H.-K. Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images," *Pattern Recognition*, vol. 42, no. 11, pp. 3083–3096, 2009.

[28] T. Gao, Z. Chen, Z. Yuan, and G. Chen, "A hyperchaos generated from Chen's system," *International Journal of Modern Physics C*, vol. 17, no. 4, pp. 471–478, 2006.