Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 940638, 9 pages
http://dx.doi.org/10.1155/2015/940638

Research Article

Medical Image Encryption and Compression Scheme Using Compressive Sensing and Pixel Swapping Based Permutation Approach

Li-bo Zhang,[1,2] Zhi-liang Zhu,[1] Ben-qiang Yang,[2] Wen-yuan Liu,[2] Hong-feng Zhu,[2] and Ming-yu Zou[2]

[1]*Software College, Northeastern University, Shenyang 110004, China*
[2]*Department of Radiology, The General Hospital of Shenyang Command PLA, Shenyang 110016, China*

Correspondence should be addressed to Zhi-liang Zhu; zhuzhiliang.sc@gmail.com

Received 13 May 2015; Revised 12 July 2015; Accepted 13 July 2015

Academic Editor: Kishin Sadarangani

This paper presents a solution to satisfy the increasing requirements for secure medical image transmission and storage over public networks. The proposed scheme can simultaneously encrypt and compress the medical image using compressive sensing (CS) and pixel swapping based permutation approach. In the CS phase, the plain image is compressed and encrypted by chaos-based Bernoulli measurement matrix, which is generated under the control of the introduced Chebyshev map. The quantized measurements are then encrypted by permutation-diffusion type chaotic cipher for the second level protection. Simulations and extensive security analyses have been performed. The results demonstrate that at a large scale of compression ratio the proposed cryptosystem can provide satisfactory security level and reconstruction quality.

1. Introduction

Benefiting from the rapid developments of network technologies and prominent advantages of digital medical images in health protection [1], the increasing distribution of medical images over networks has been an essential of everyday life in medical systems. As medical images are the confidential data of patients, how to ensure their secure storage and transmission over public networks has therefore become a critical issue of practical medical applications. Mandates for ensuring health data security have been issued by the federal government, such as Health Insurance Portability and Accountability Act (HIPAA), enacted by the United states Congress and signed by president Bill Clinton in 1996 [2, 3]. Moreover, several major medical imaging communities such as American College of Radiology (ACR) have issued guidelines and mandates for ensuring medical image security, for example, the Picture Archiving and Communication Systems (PACS) [4]. However, transmission of medical image of PACS is generally within a hospital intranet whose security measures or instruments are often lacking [3]. Except for the intranet environment, medical images transmission over wireless networks is also in an increasing demand. Medical image security in both intranet and internet faces severe threats [5].

Encryption is the most convenient strategy to guarantee the security of medical images over public networks. However, recent achievements have demonstrated that block ciphers such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA), which are originally designed for encrypting textual data, are poorly suited for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [6–8]. Since 1990s, chaotic systems have drawn much attention as their fundamental features such as ergodicity, unpredictability, and sensitivity to initial system parameters can be considered analogous to some ideal cryptographic properties for image encryption [9]. In 1998, Fridrich proposed the first general architecture for chaos-based image cipher. This architecture is composed of two stages: permutation and diffusion [10]. Under

this structure, a plain image is firstly shuffled by a two-dimensional area-preserving chaotic map in the permutation stage, with the purpose to erase the high correlation between adjacent pixels. Then the pixel values are modified sequentially using pseudorandom key stream elements produced by a certain qualified chaotic map in the diffusion procedure. During the past decades or so, researchers have performed extensive analyses to this architecture, and the improvements are subsequently proposed [11–19]. The improvements lie in various aspects, such as novel permutation approaches [12–14], improved diffusion schemes [15, 16], and enhanced key stream generators [17–19]. Chaos-based ciphers have also been employed for medical applications [20, 21]. In [20], a chaos-based visual encryption mechanism for clinical electroencephalography signals is developed, whereas a bit-level medical image encryption scheme is built in [21]. Besides the chaos-based encryption, compressive sensing (CS) [22, 23] is also found to be a feasible way to build cryptosystems, where the sensing matrix can be viewed as the secret key [24]. It is suggested by Rachlin and Baron that CS can guarantee computational secrecy [25]. In [26, 27] Zhou et al. proposed combining chaos theory with CS and then building two secure image encryption schemes, whereas the quantization process is ignored. In [28], researchers proposed a joint quantization and diffusion approach based on the similarities between error feedback mechanism of the quantizer and cryptographic diffusion primitive.

In this paper, a medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach is proposed. The whole process consists of two stages, where the first one is the chaos-based CS procedure that is used to compress and provide the first level protection, while the second procedure is a chaos-based permutation-diffusion encryption module. Chaotic Chebyshev map is employed to generate the Bernoulli sensing matrix for CS, and then it is reused in the second stage to produce the permutation key stream elements. In the diffusion procedure, logistic map is introduced to generate the key stream to mask the plaintext. Simulations and extensive security analyses both demonstrate that the proposed scheme has satisfactory security and compression performances for practical medical applications. The proposed scheme will be given out in detail in the next section; simulations results and security analyses are carried out in Section 3. Finally, conclusions will be drawn in the last section.

2. The Proposed Scheme

2.1. CS with Cryptographic Features Embedded. The CS is a new framework for simultaneous sampling and compression of signals. For a length_N signal x, it is said to be K-sparse if x can be well approximated using only K coefficients under some linear transform $x = \Psi s$, where Ψ is the sparsifying basis and s is the transform coefficient vector with at most $K \ll N$ (significant) nonzero entries. Many natural signals are sparse or compressible, such as the smooth signals which are compressible in the Fourier basis, whereas natural images are mostly compressible in a wavelet or discrete cosine transform (DCT) basis. In CS, the signal is measured not via standard point samples but rather through the projection by a linear measurement matrix Φ:

$$y = \Phi x = \Phi\Psi s = \Theta s, \tag{1}$$

where y is the sampled vector with $M \ll N$ data points and Φ represents $M \times N$ acquisition matrix. The CS framework is attractive as it implies that x can be faithfully recovered from only $M = O(K \log N)$ measurements, suggesting the potential of significant cost reduction in data acquisition [29]. Unlike the random linear projection in the sampling process, the signal recovery process from the received measurements y is highly nonlinear. When Θ satisfies the restricted isometry property (RIP), the reconstruction can be preceded by solving the following ℓ_1-norm minimization problem [30]:

$$\begin{aligned} \min \quad & \|s\|_1 \\ \text{s.t.} \quad & \Theta s = y. \end{aligned} \tag{2}$$

At the receiver end, convex optimization algorithms [22, 23] or greedy pursuit method such as Orthogonal Matching Pursuit (OMP) [31] can be employed for reconstruction.

The popular family of the measurement matrices is a random projection or a matrix of random variables, such as Gaussian or Bernoulli matrices. This family of measurement matrices is well known as it is universally incoherent with all other sparsifying bases, which is crucial for satisfying the RIP requirement. In our scheme, Bernoulli matrix as shown in (3) is introduced for signal projection. Here, $\Phi_{i,j}$ $(i \le M, j \le N)$ represents the entry of the $M \times N$ measurement matrix, and it has values $\pm 1/\sqrt{M}$ with signs chosen independently and uniformly distributed:

$$\Phi_{i,j} = \frac{1}{\sqrt{M}} \begin{cases} 1 & P = \frac{1}{2} \\ -1 & P = \frac{1}{2}. \end{cases} \tag{3}$$

As pointed out in [29], one of the challenging issues of CS in practice is to design a measurement matrix that satisfies (1) optimal sensing performance; (2) universality with almost all sparsifying basis; (3) low complexity; and (4) hardware/optics implementation friendliness. Traditional Bernoulli matrices meet the first two requirements whereas it is costly to generate, store, and transmit in practice. As a result, it is preferable to generate and handle the measurement matrix by one or more seed keys only. In this paper, we propose to construct the measurement matrix using chaotic Chebyshev map, as described in (4), where k and x_n are the control parameter and state value, respectively. As can be seen, the iteration results of Chebyshev map fall within $[-1, 1]$:

$$x_{n+1} = T_k(x_n) = \cos\left(k \cdot \cos^{-1} x_n\right), \quad x_n \in [-1, 1]. \tag{4}$$

For $\Phi_{i,j}$ $(i \le M, j \le N)$, the Chebyshev map will iterate once and then be quantized to the required format of $\Phi_{i,j}$ by (5). In this strategy, the measurement matrix is under the control of chaotic sequence, which is generated by chaotic

(a) (b) (c)

Figure 1: Simulation results of PSP: (a) the plaintext; (b) 1 round shuffled image; (c) 2 rounds shuffled image.

system with initial values and particular control parameter. In short, control parameter k and initial state value x_0 can be combined as the keys. This facilitates the transmission and sharing that only requires a few values instead of the whole measurement matrix:

$$\Phi_{i,j} = \begin{cases} 1 & \text{if } (x_n \geq 0) \\ -1 & \text{if } (x_n \leq 0) \end{cases} \quad (5)$$

$$n = j + i \times N.$$

The use of CS for security purposes was first outlined in [24], where it is suggested that the measurements obtained from random linear projections can be treated as ciphertext as the attacker cannot decode it unless he knows in which random subspace the coefficients are expressed. Then in [32, 33], it is investigated that the Shannon perfect secrecy is, in general, not achievable by such a CS method while computational security can be achieved. In the proposed scheme, with the introduction of Chebyshev map, the CS is regarded as a joint encryption and compression procedure.

2.2. Pixel Swapping Based Permutation Strategy. In traditional image permutation techniques, pixels are generally scrambled by a two-dimensional area-preserving chaotic map, without any modification to their values. Three types of chaotic maps, Arnold cat map, standard map, and baker map, are always employed [7, 9, 18]. All pixels are scanned sequentially from upper-left corner to lower-right corner, and then the confused image is produced. However, such permutation maps cannot be used for the proposed scheme. That is because the CSed image is generally not a square one. As pointed out in [7], Arnold cat map, standard map, and baker map are merely suitable for shuffling square images. When confusing a nonsquare plain image, extra pixels have to be padded to construct a square image firstly, and that would downgrade the efficiency of the cryptosystem.

Regarding this, a novel pixel swapping based permutation strategy (PSP) is developed for shuffling nonsquare images. In PSP, pixels of the plaintext and the ciphertext are represented by $P = \{P(1), P(1), \ldots, P(M \times N)\}$ and $C = \{C(1), C(1), \ldots, C(M \times N)\}$ from left to right, top to bottom, respectively. Each pixel in the plain image will be swapped with another pixel located after it, whose position is determined by a pseudorandom number acting as current key stream element. Suppose that X is the current pixel position and X' is the coordinate of the corresponding swapped pixel. The coordinate X' is calculated according to (6), where $k_c(X)$ is current permutation key stream element. In PSP, $k_c(X)$ is obtained from the Chebyshev state variables produced in the CS procedure, the production formula is described in (7), where floor(x) returns the value nearest integers less than or equal to x, and mod(x, y) returns the remainder after division. In collaboration with (6), PSP can ensure that all of the pixels swapping operations are performed within the valid region:

$$X' = X + k_c(X), \quad (6)$$

$$k_c(n) = \operatorname{mod}\left[\operatorname{floor}\left(\operatorname{abs}(x(n)) \times 10^{15}\right), M \times N - X\right] + 1. \quad (7)$$

Simulations have been performed to verify the image permutation performance of PSP; the results are demonstrated in Figure 1. The plaintext is shown in Figure 1(a), which is a deliberately customized CT image with size of 256 × 512 for PSP evaluation. Figures 1(b) and 1(c) are the shuffled images using 1 round and 2 rounds of PSP, respectively. Obviously, the permutated images are completely unrecognizable and with no similarity with the plaintext, which means the plaintext has been effectively encrypted. Besides, the noise-like two images are of less difference with each other. In practice, one round is sufficient to hide the plain information and reduce the pixel correlation of the plain image, as the preferred case in our scheme illustrated in the next subsection.

2.3. Schematic of the Proposed System. The schematic of proposed medical image encryption and compression system is shown in Figure 2. As can be seen, the proposed system consists of two primary procedures. The first one is the CS module with cryptographic features embedded, which is used to compress the plaintext and simultaneously provided the first level encryption, with the initial value and control parameter of the introduced Chebyshev map serving as the secret key. The subsequent procedure is a permutation-diffusion type image cipher, which will extensively encrypt the quantized measurements produced in the CS stage. Obviously, the latter procedure is an iterative module, in which PSP is employed for image permutation. Following the PSP is a typical diffusion operation as illustrated in (8), in which $p(n)$, $k(n)$, $c(n)$, and $c(n-1)$ represent the current plain pixel, key stream element, output cipher-pixel, and the previous cipher-pixel, respectively. The key stream element $k(n)$ used for masking is calculated by (9), where $x(n)$ is the current state of the chaotic map:

$$c(n) = k(n) \oplus p(n) \oplus c(n-1), \quad (8)$$

$$k(n) = \operatorname{mod}\left[\operatorname{floor}\left(x(n) \times 10^{15}\right), 256\right]. \quad (9)$$

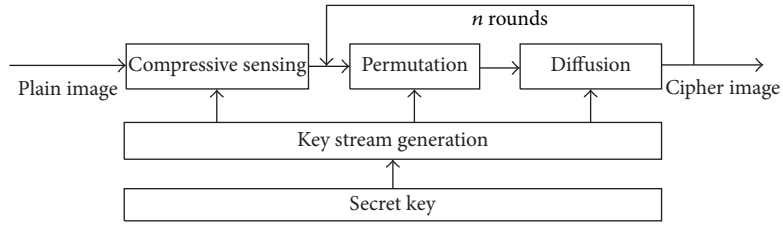

Figure 2: The schematic of the proposed system.

Chaotic logistic map is employed in our scheme for the generation of $x(n)$, which is described by

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \tag{10}$$

where μ and x_n are the control parameter and state value, respectively. If one chooses $\mu \in [3.57, 4]$, the system is chaotic. The initial value x_0 and control parameter μ combine as the secret key. Here notice that there exist some periodic (nonchaotic) windows in chaotic region of logistic map. To address this problem, values corresponding to positive Lyapunov exponents should be selected for parameter μ, so as to keep the effectiveness of the cryptosystem [21].

The operation procedures of the proposed scheme can be described as follows.

Step 1. Iterate (4) with (k, x_0) for N_0 times to avoid the harmful effect of transitional procedure, where N_0 is a constant.

Step 2. Iterate (4) $N \times N$ times, and generate the measurement matrix Φ using (5). Besides, for the first $M \times N$ iterations, get the permutation key stream elements simultaneously according to (7).

Step 3. Compressive sample the plaintext according to $y = \Phi x$.

Step 4. Quartzite the measurement data y through Lloyd quantizer, which is known as an optimal quantizer in the mean square error sense.

Step 5. Confuse the quartzited data according to (6) and (7), with the help of the permutation key stream elements produced in the second step.

Step 6. Iterate (10) with (μ, x_{02}) for N_0 times to avoid the harmful effect of transitional procedure constant.

Step 7. Iterate (10) continuously for $M \times N$ times. For each iteration, obtain a diffusion key stream element according to (9).

Step 8. Calculate the cipher-pixel value using (8). For the first pixel, an initial value $c(-1)$ can be set as a seed.

Step 9. Repeat Steps 5–8 to satisfy the security requirement.

3. Simulations and Security Analyses

In this section, simulation results of the proposed encryption and compression scheme are given out for validation. Four medical images with size 512×512 are introduced as plaintexts, as shown in the first column of Figure 3, named as CT_Abdomen, CT_Paranasal_sinus, MR_Knee, and X_Lungs, respectively. The reconstruction algorithm for the CS module is OMP [31], and the sparsifying basis is discrete wavelet transform. The compression ratio is 0.5 for demonstration, which means $M = 256$. The algorithm is simulated in Matlab R2010a platform, and the secret key is random selected as $k = 5.782595812953629$, $x_0 = 0.236925687412914$ for Chebyshev map, and $\mu = 3.999345672564248$, $x_{02} = 0.256799133578126$ for logistic map.

3.1. Encryption Results. The results are shown in Figure 3, with the plaintexts and ciphertexts depicted in the first and third column, respectively. It is obvious that the volumes of the ciphertexts have been compressed half compared with those of the plaintexts. Besides, the ciphertexts are noise-like and unrecognizable from visual perception. We further verify the randomness of the ciphertexts from the statistical perspective. The histograms of the corresponding plaintexts are illustrated in the second column, whereas those of the ciphertexts are shown in the fourth column. Comparatively, the histograms of the ciphertexts are uniformly distributed and quite different from those of the plain images, which indicate that the redundancy of the plain image has been successfully hidden after the encryption and consequently does not provide any clue to apply statistical attacks.

In the receiver end, we use OMP to reconstruct the plaintexts; the recovered images are illustrated in the fifth column of Figure 3. From visual perception, one can observe that the recovered images are of meaningful information and there is no notable quality degradation compared with the plaintexts. We compute the Peak Signal Noise Ratio (PSNR) as a numerical objective metric to evaluate the reconstruction quality. Under the compression ratio of 0.5 as shown in Figure 3, the recovered images are with PSNRs 33.8968 dB, 34.9182 dB, 36.7858 dB, and 36.1887 dB, respectively. All of the PSNRs exceeded 30 dB, which implies that the reconstruction quality was acceptable. From 0.1 to 0.9, PSNRs under different compression ratios are plotted in Figure 4, from which one can see that the PSNR can exceed 30 dB when the compression ratio is greater than 0.3. In practical medical

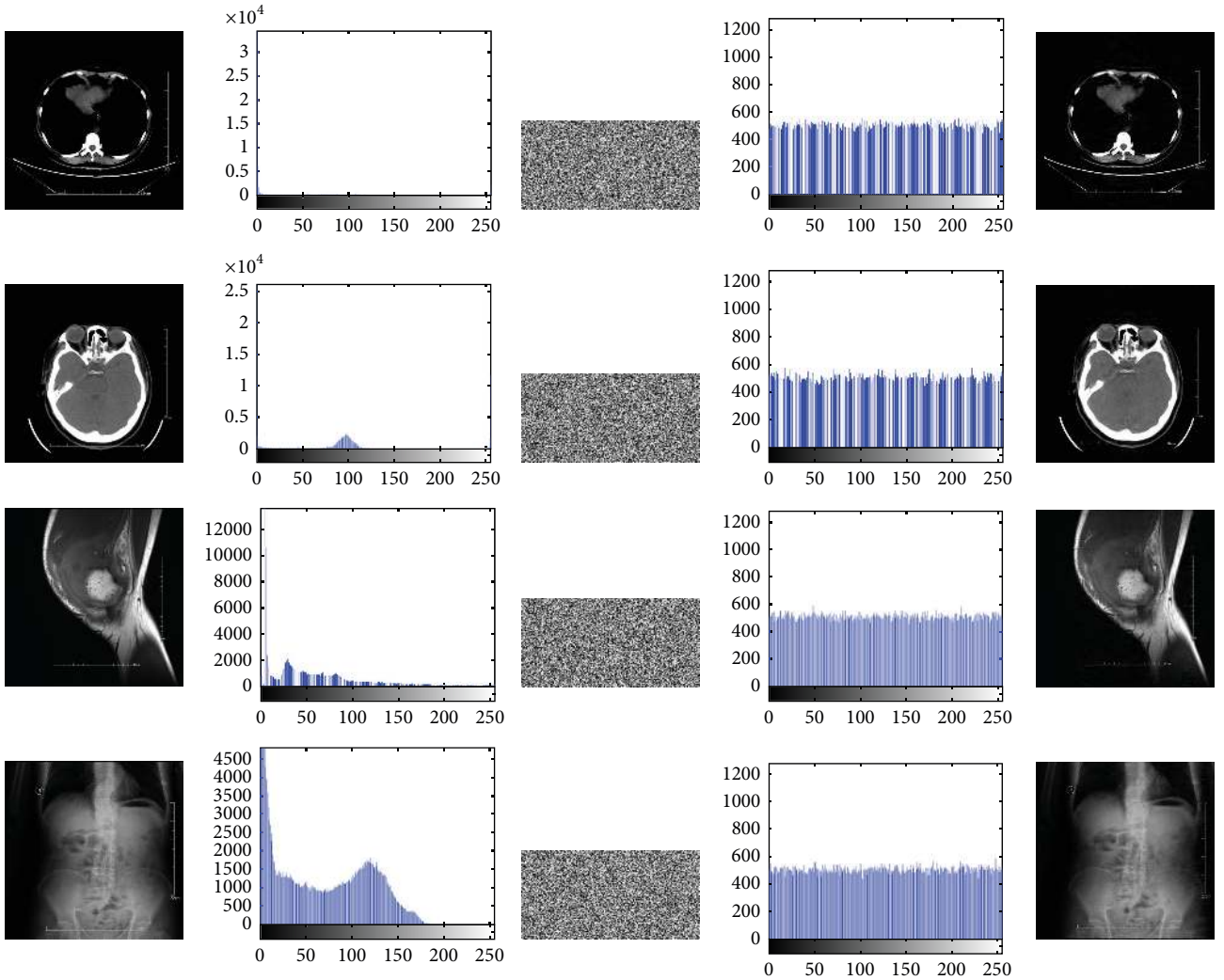

Figure 3: Simulation results of the proposed scheme: from the first to the fifth column are plaintext, histogram of the plaintext, ciphertext, histogram of the ciphertext, and the recovered images, respectively.

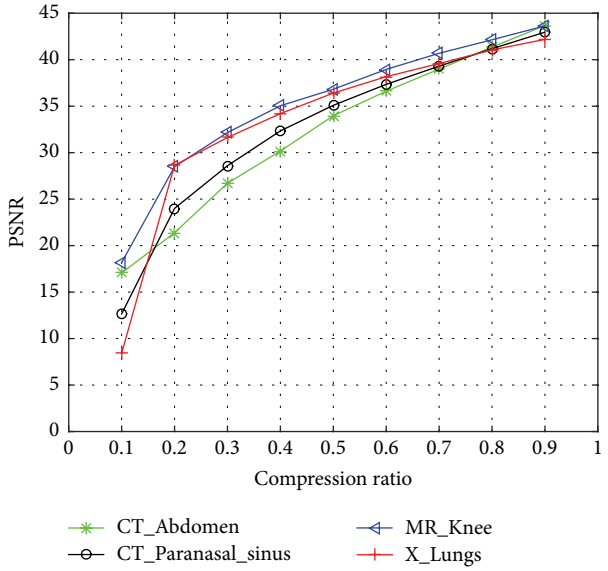

Figure 4: PSNR plot of different compression ratios.

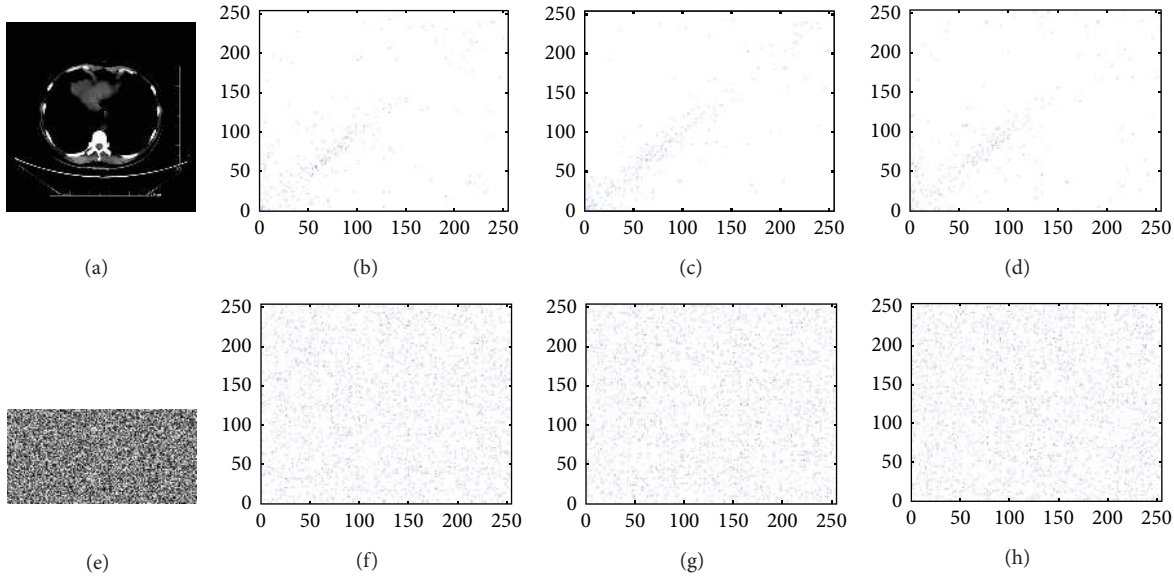

Figure 5: Correlation plots of adjacent two pixels: (a) plain image, correlation plots of the plain image in (b) horizontal, (c) vertical, (d) and diagonal directions; (e) cipher image, correlation plots of the cipher image in (f) horizontal, (g) vertical, (h) and diagonal directions.

applications, there is a large scale for the compromise between compression ratio and recovery quality.

3.2. Key Space Analysis. The key space size is the total number of different keys that can be used in a cryptosystem. For an effective cryptosystem, key space should be large enough to make brute-force attack infeasible. In the proposed scheme, the keys consist of the initial value $x_0 \in (-1, 1)$ and control parameter $k \in [2, +\infty)$ of Chebyshev map and the initial value $x_0 \in (0, 1)$ and control parameter $\mu \in (3.57, 4]$ of logistic map. It should be noted that k should be restricted to a particular interval of 2π to prevent Chebyshev map from producing periodic orbits. According to the IEEE floating-point standard [34], the computational precision of the 64-bit double-precision number is about 10^{-15}. The total key space of the proposed scheme is

$$\begin{aligned} \text{Key} &= 2 \times 10^{15} \times 2\pi \times 10^{15} \times 10^{15} \times 0.43 \times 10^{15} \\ &= 5.4 \times 10^{60} \approx 2^{202}, \end{aligned} \tag{11}$$

which is large enough to resist brute-force attack.

3.3. Pixel Correlation Analysis. For a medical image with meaningful visual content, each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical, or diagonal directions. An effective cryptosystem should produce ciphertexts with sufficiently low correlation between adjacent pixels. The following steps are performed to evaluate an image's correlation property. (1) 3000 pixels are randomly selected as samples; (2) the correlations between two adjacent pixels in horizontal, vertical, and diagonal directions are calculated according to (12), where x_i and y_i are gray-level values of the ith pair of the selected adjacent pixels, and N represents the total number of the samples:

$$\begin{aligned} r_{xy} &= \frac{E\left(x - E\left(x\right)\right)\left(y - E\left(y\right)\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}}, \\ E\left(x\right) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D\left(x\right) &= \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\left(x\right)\right)^2. \end{aligned} \tag{12}$$

Table 1: Correlation coefficients of adjacent pixels.

Direction	Plain image	Cipher image
Horizontal	0.9218	−0.0131
Vertical	0.9605	−0.0084
Diagonal	0.8891	−0.0180

The correlation coefficients of adjacent pixels in the plain image and its cipher image are listed in Table 1. Furthermore, the correlation plots of two adjacent pixels are depicted in Figure 5. The high correlation of adjacent plain pixels can be observed in Figures 5(b), 5(c), and 5(d), as the dots are located along the diagonal. They are scattered over the entire plane in Figures 5(f), 5(g), and 5(h), which reflect the correlations of the ciphertext. Both the calculated correlation coefficients and the figures can substantiate that the strong correlation among neighboring pixels of a plain image can be effectively decorrelated by the proposed cryptosystem.

3.4. Key Sensitivity Test. Extreme key sensitivity is a crucial feature of an effective cryptosystem and can be evaluated in

Table 2: Differences between cipher images produced by slightly different keys.

Figures	Encryption keys				Differences with Figure 6(b)
	k	x_0	μ	x_{02}	
Figure 6(b)	5.782595812953629	0.236925687412914	3.999345672564248	0.256799133578126	—
Figure 6(c)	5.782595812953630	0.236925687412914	3.999345672564248	0.256799133578126	99.5941%
Figure 6(e)	5.782595812953629	0.236925687412915	3.999345672564248	0.256799133578126	99.5934%
Figure 6(g)	5.782595812953629	0.236925687412914	3.999345672564249	0.256799133578126	99.6147%
Figure 6(i)	5.782595812953629	0.236925687412914	3.999345672564248	0.256799133578127	99.6124%

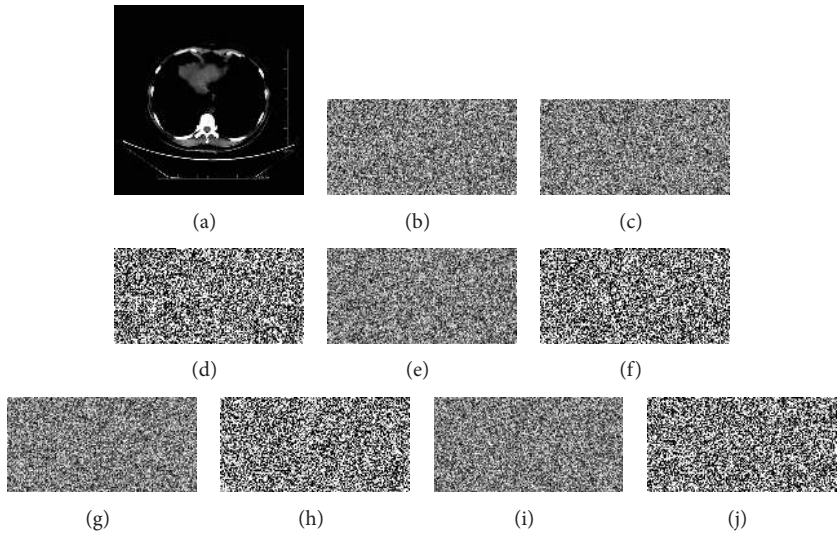

Figure 6: Key sensitivity test in the first case: (a) plain image; (b) cipher image (k = 5.782595812953629, x_0 = 0.236925687412914, μ = 3.999345672564248, and x_{02} = 0.256799133578126); (c) cipher image (k = 5.782595812953630, x_0 = 0.236925687412914, μ = 3.999345672564248, and x_{02} = 0.256799133578126); (d) differential image between (b) and (c); (e) cipher image (k = 5.782595812953629, x_0 = 0.236925687412915, μ = 3.999345672564248, and x_{02} = 0.256799133578126); (f) differential image between (b) and (e); (g) cipher image (k = 5.782595812953629, x_0 = 0.236925687412914, μ = 3.999345672564249, and x_{02} = 0.256799133578126); (h) differential image between (b) and (h); (i) cipher image (k = 5.782595812953629, x_0 = 0.236925687412914, μ = 3.999345672564248, and x_{02} = 0.256799133578127); (j) differential image between (b) and (i).

two aspects: (i) completely different ciphertexts should be produced when slightly different keys are used to encrypt the same plaintext; (ii) the ciphertext cannot be correctly decrypted even if tiny mismatch exists between the encryption and decryption keys.

To evaluate the key sensitivity of the first case, the encryption is carried out with a randomly chosen secret key to obtain a cipher image. Then a slight change 10^{-15} is introduced to one of the parameters while all others remain unchanged, and repeat the encryption process. The corresponding cipher images and differential images are shown in Figure 6. The differences between the corresponding cipher images are computed and listed in Table 2. It is clear that a tiny difference in the secret key causes substantial changes between the corresponding cipher images.

Furthermore, decryption using keys with slight alternations as described previously has also been performed, so as to evaluate the key sensitivity of the second case. The decipher images are shown in Figure 7. It is obvious that all of the incorrect decipher images are completely unrecognizable and cannot reveal any perceptive information of the plaintext, which demonstrated the failure of reconstruction when using a neighbor key.

3.5. Entropy Analysis. Information entropy is a significant property that reflects the randomness and the unpredictability of an information source. It was firstly proposed by Shannon in 1949, and the entropy $H(s)$ of a message source s is defined in (13), where s is the source, N is the number of bits to represent the symbol s_i, and $P(s_i)$ is the probability of the symbol s_i. For a truly random source consisting of 2^N symbols, the entropy is N. Therefore, for a secure cryptosystem, the entropy of the cipher image with 256 gray levels should ideally be 8:

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i). \tag{13}$$

The entropies of the introduced medical images and their ciphertexts are listed in Table 3. It is obvious that the entropies of the cipher images are very close to the theoretical value of 8, which means that the information leakage in the encryption

Table 3: Entropies of plain images and cipher images.

Test images	Plain images	Cipher images
CT_Abdomen	1.675035	7.9983
CT_Paranasal_sinus	3.328586	7.9986
MR_Knee	5.384937	7.9984
X_Lungs	6.966350	7.9986

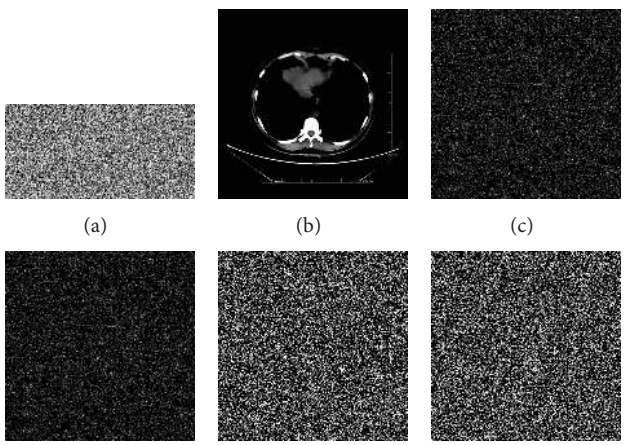

Figure 7: Key sensitivity test in the second case: (a) cipher image (k = 5.782595812953629, and x_0 = 0.236925687412914, μ = 3.999345672564248, x_{02} = 0.256799133578126); (b) decipher image with correct keys; (c) decipher image (k = 5.782595812953630, x_0 = 0.236925687412914, μ = 3.999345672564248, and x_{02} = 0.256799133578126); (d) decipher image (k = 5.782595812953629, x_0 = 0.236925687412915, μ = 3.999345672564248, and x_{02} = 0.256799133578126); (e) decipher image (k = 5.782595812953629, x_0 = 0.236925687412914, μ = 3.999345672564249, and x_{02} = 0.256799133578126); (f) decipher image (k = 5.782595812953629, x_0 = 0.236925687412914, μ = 3.999345672564248, and x_{02} = 0.256799133578127).

procedure is negligible and the proposed cryptosystem is secure against entropy attack.

4. Conclusions

In this paper, a medical image encryption and compression scheme has been proposed. We employed compressive sensing to firstly compress and encrypt the plaintext, and the measurement matrix is generated using chaotic Chebyshev map. Then the quantized measurements are subsequently encrypted using chaos-based permutation-diffusion cipher to further enhance the security. Simulations and security analyses have demonstrated the satisfactory compression and encryption performances of the proposed scheme.

Conflict of Interests

The authors declare no conflict of interests.

Acknowledgment

This work was supported by Programs for Science and Technology Development of LiaoNing Province (no. 2013225036-13, Research on Regional Collaborative Medical Imaging Information Platform; no. 2013225089, Research on Imaging of Children's Congenital Heart Disease Using Multi-Slice CT).

References

[1] D.-C. Lou, M.-C. Hu, and J.-L. Liu, "Multiple layer data hiding scheme for medical images," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 329–335, 2009.

[2] United States Department of Health and Human Services, HIPPA: medical privacy–national standards to protect the privacy of personal health information, http://www.hhs.gov/ocr/privacy/.

[3] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, no. 2-3, pp. 185–196, 2003.

[4] C. Fu, G.-Y. Zhang, O. Bian, W.-M. Lei, and M. Hong-feng, "A novel medical image protection scheme using a 3-dimensional chaotic system," *PLoS ONE*, vol. 9, no. 12, Article ID e115773, 2015.

[5] L. B. Zhang, Z. L. Zhu, B. Q. Yang, W. Y. Liu, H. F. Zhu, and M. Y. Zou, "Cryptanalysis and improvement of an efficient and secure medical image protection scheme," *Mathematical Problems in Engineering*, vol. 2015, Article ID 913476, 11 pages, 2015.

[6] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism," *Optics Express*, vol. 21, no. 23, pp. 27873–27890, 2013.

[7] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "A fast image encryption scheme with a novel pixel swapping-based confusion approach," *Nonlinear Dynamics*, vol. 77, no. 4, pp. 1191–1207, 2014.

[8] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, chapter 4, CRC Press, 2005.

[9] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and L.-B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 3, pp. 846–860, 2015.

[10] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[11] Y. Zhang and D. Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption," *AEU*, vol. 68, no. 4, pp. 361–368, 2014.

[12] C. Fu, J.-B. Huang, N.-N. Wang, Q.-B. Hou, and W.-M. Lei, "A symmetric chaos-based image cipher with an improved bit-level permutation strategy," *Entropy*, vol. 16, no. 2, pp. 770–788, 2014.

[13] X. Zhang and X. Wang, "Chaos-based partial encryption of SPIHT coded color images," *Signal Processing*, vol. 93, no. 9, pp. 2422–2431, 2013.

[14] Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74–82, 2014.

[15] X.-J. Tong, "The novel bilateral—diffusion image encryption algorithm with dynamical compound chaos," *Journal of Systems and Software*, vol. 85, no. 4, pp. 850–858, 2012.

[16] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[17] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Communications in Nonlinear Science and Numerical Simulation*, vol. 23, no. 1–3, pp. 294–310, 2015.

[18] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using a chaotic Baker map and double random phase encoding," *Journal of Optics*, vol. 16, no. 12, Article ID 125403, 2014.

[19] X. Tong and M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," *Signal Processing*, vol. 89, no. 4, pp. 480–491, 2009.

[20] C.-F. Lin, C.-H. Chung, and J.-H. Lin, "A chaos-based visual encryption mechanism for clinical EEG signals," *Medical and Biological Engineering and Computing*, vol. 47, no. 7, pp. 757–762, 2009.

[21] C. Fu, W.-H. Meng, Y.-F. Zhan et al., "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000–1010, 2013.

[22] E. J. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[23] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[24] E. J. Candes and T. Tao, "Near-optimal signal recovery from random projections: universal encoding strategies?" *IEEE Transactions on Information Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.

[25] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proceedings of the 46th Annual Allerton Conference on Communication, Control, and Computing*, pp. 813–817, Urbana-Champaign, Ill, USA, September 2008.

[26] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Optics & Laser Technology*, vol. 62, pp. 152–160, 2014.

[27] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression-encryption algorithm based on compressive sensing," *Optik*, vol. 125, no. 18, pp. 5075–5080, 2014.

[28] L. Zhang, K. W. Wong, Y. Zhang, and Q. Lin, "Joint quantization and diffusion for compressed sensing measurements of natural images," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '15)*, pp. 2744–2747, Lisbon, Portugal, May 2015.

[29] T. T. Do, L. Gan, N. H. Nguyen, and T. D. Tran, "Fast and efficient compressive sensing using structurally random matrices," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 139–154, 2012.

[30] H. Fang, S. A. Vorobyov, H. Jiang, and O. Taheri, "Permutation meets parallel compressed sensing: how to relax restricted isometry property for 2D sparse signals," *IEEE Transactions on Signal Processing*, vol. 62, no. 1, pp. 196–210, 2014.

[31] J. A. Tropp and A. C. Gilbert, "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[32] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *Proceedings of the IEEE Military Communications Conference (MILCOM '08)*, pp. 1–7, San Diego, Calif, USA, November 2008.

[33] S. A. Hossein, A. E. Tabatabaei, and N. Zivic, "Security analysis of the joint encryption and compressed sensing," in *Proceedings of the 20th Telecommunications Forum (TELFOR '12)*, pp. 799–802, Belgrade, Serbia, November 2012.

[34] IEEE Computer Society, "IEEE standard for binary floating-point arithmetic," ANSI/IEEE Standard 754-1985, 1985.