Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2015, Article ID 913476, 11 pages
http://dx.doi.org/10.1155/2015/913476

Research Article

Cryptanalysis and Improvement of an Efficient and Secure Medical Image Protection Scheme

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 26 August 2014; Accepted 25 November 2014

Academic Editor: Jonathan N. Blakely

Nowadays, the increasing demand for telemedicine services has raised interest in the real-time medical image protection literatures. In this paper, we evaluate the security of an efficient and secure medical image protection scheme recently proposed (Fu et al., 2013). It is found that this scheme can be successfully broken by launching chosen-plaintext attacks. Improvement is subsequently developed for promoting the security and efficiency performance. Extensive security analyses and experimental results both indicate that the improved scheme can well address the security flaws and advance the speed performance of the original one.

1. Introduction

With the dramatic development of communication technologies and the significant advantages of digital medical images in health protection [1], the increasing demand for distribution of digital medical images over networks has become an essential part of everyday life in medical systems. Medical image security is therefore becoming an important issue when digital images and their pertinent patient information are stored and transmitted across public networks [1–4]. 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 in 1996 [5, 6]. Guidelines such as picture archiving and communication systems (PACS) as well as digital imaging and communications in medicine (DICOM) standard that deals with security issues continue to be published by organizing bodies in healthcare [7]. However, transmission of medical data in a PACS environment is generally within a hospital intranet, and these security measures or instruments are often lacking [5]. Except for the intranet environment, medical images transmission over wireless networks is also an increasing requirement. Medical image security in both intranet and internet faces sever threats.

Encryption is the most convenient and useful approach to guarantee the data security during its storage and transmission over public networks. However, block ciphers such as data encryption standard (DES), advanced encryption standard (AES), and international data encryption algorithm (IDEA) that are originally designed for encrypting textual data have been found poorly suited for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [8]. Throughout the researchers' long-term efforts, a variety of chaos-based image encryption schemes have been built for real-time and secure image transmission [9–21]. Meanwhile, recent cryptanalysis works have demonstrated that some of the chaos-based image cryptosystems are insecure against various attacks and have been successfully broken [22–28]. The weaknesses in these insecure cryptosystems primary lie in two aspects. (1) In these cryptosystems, permutation and substitution are generally two independent procedures, in which case the confusion effect can be removed under chosen-plaintext attack using a homogeneous image with identical pixels. (2) The key stream is completely depending on the secret key, which allows

attackers to launch known-plaintext or chosen-plaintext attacks so as to retrieve the equivalent key stream elements. Some general rules for evaluating the security performance of chaos-based cryptosystems can be found in [29].

In [30], an efficient and secure medical image protection scheme was proposed, using bit-level chaos-based image encryption techniques. Simulation results have proved that the scheme is much more efficient than DES. This renders it as a suitable candidate for real-time medical image encryption. In the present paper, we evaluate the security of this scheme. It is found that both the weaknesses abovementioned exist in this algorithm, and this scheme shows vulnerability to chosen-plaintext attack. The equivalent substitution key stream elements can be retrieved by using only one chosen-plaintext, whereas the permutation matrix will be recovered by using at least 18 chosen plaintexts for a 512 × 512 plain image. On the basis of the cryptanalysis achievement, corresponding improvement is subsequently proposed for enhancing the security and further accelerating the encryption speed. Simulations have proved that the vulnerability to chosen-plaintext attack of the original scheme is well addressed and more satisfactory encryption efficiency can be obtained simultaneously when using the improved scheme.

The remainder of this paper is organized as follows. Section 2 briefly introduces the medical image encryption scheme under study. An effective chosen-plaintext attack and the corresponding improvement of the original scheme are reported in Section 3. Thorough security analyses of the improved scheme are carried out in Section 4. Finally, conclusions will be drawn in Section 5.

2. The Medical Image Encryption Scheme under Study

The permutation-substitution architecture, which was firstly proposed by Fridrich in 1998 [9] and has been widely used for building chaos-based image cryptosystems, was employed in this scheme. The schematic of the cryptosystem is shown in Figure 1.

Under this structure, a plain image is firstly shuffled using Arnold cat map based bit-level permutation technique, and then pixel values are modified sequentially with the help of pseudorandom key stream elements produced by chaotic logistic map in the substitution procedure. Three-round bit-level permutation in a single encryption round and two rounds overall encryption is suggested in the original paper.

In order to simultaneously achieve image confusion performance and pixel value modification effect in the permutation stage, a novel bit-level image permutation strategy is proposed in this scheme. For bit-plane decomposition, each pixel with 256 gray-levels is regarded as a bit sequence

$$P(x, y) = b(7)\, b(6)\, b(5) \cdots b(0), \tag{1}$$

where $P(x, y)$ is the value of the pixel at coordinate (x, y) and the number in parentheses indicates the bit index from highest bit 7 to the lowest bit 0. Consequently, we can decompose a 256 gray-level image into 8 independent bit planes and each bit plane is a binary image because there are only two possible intensity values (0 and 1) for each pixel. Taking a 256 gray-level CT image for example, its bit planes are demonstrated in Figure 2.

Then each of the bit planes is shuffled independently using Arnold cat map with different control parameters. The generalized Arnold cat map and its inverse transform are defined in (2), where p and q are control parameters, x, y, x', y' are the pixel positions before and after cat mapping, and N represents the length or width of a square image, respectively. The control parameters p and q serve as the secret key of cat map, and the authors use $(p, q), (2\times p, 2\times q), \ldots, (8\times p, 8\times q)$ as the control parameters of the cat map for 1st–8th bit-planes:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N,$$
$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N. \tag{2}$$

The shuffled bit planes will be then combined together, and the permutated version of the plain image is produced. After the permutation procedure, plain pixels will be modified one by one in the substitution phase. The pixel masking equation is described in (3), 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:

$$c(n) = k(n) \oplus p(n) \oplus c(n-1). \tag{3}$$

The key stream element $k(n)$ is obtained from current state of the chaotic map according to (4), where floor (x) returns the value of x to the nearest integers less than or equal to x and L is the gray level of the plain image:

$$k(n) = \bmod \left[\text{floor}\left(x(n) \times 10^{14}\right), L\right]. \tag{4}$$

Chaotic logistic map, as described in (5), is employed for key stream generation. In (5), μ and $x(n)$ denote the control parameter and state values of logistic map, respectively. When $\mu \in [3.57, 4]$, the system is chaotic. The initial value x_0 and parameter μ serve as the secret key. Note that there exist some periodic (nonchaotic) windows in the chaotic region of logistic map. To address this problem, values corresponding to positive Lyapunov exponents should be selected for μ, so as to ensure the chaotic property of the cryptosystem:

$$x(n+1) = \mu \times x(n) \times (1 - x(n)). \tag{5}$$

3. Cryptanalysis and Improvement of the Scheme

In this section, we present the cryptanalysis and corresponding improvement of the medical image encryption scheme under study. The cryptosystem can be successfully broken using chosen-plaintext attack. Note that if the encryption is performed iteratively, the following cryptanalysis may lose effectiveness. However, considerable computation load and longer operation time are required in that circumstance,

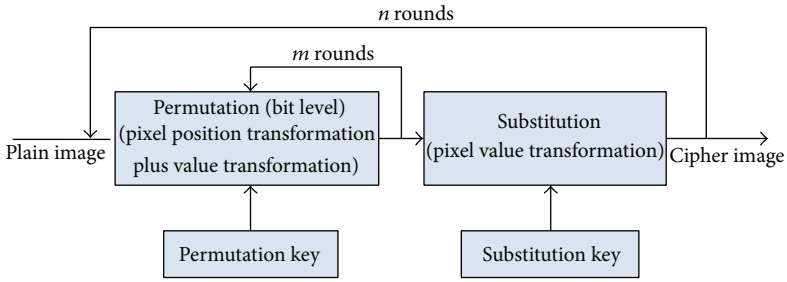


Figure 1: Architecture of the image cryptosystem under study.

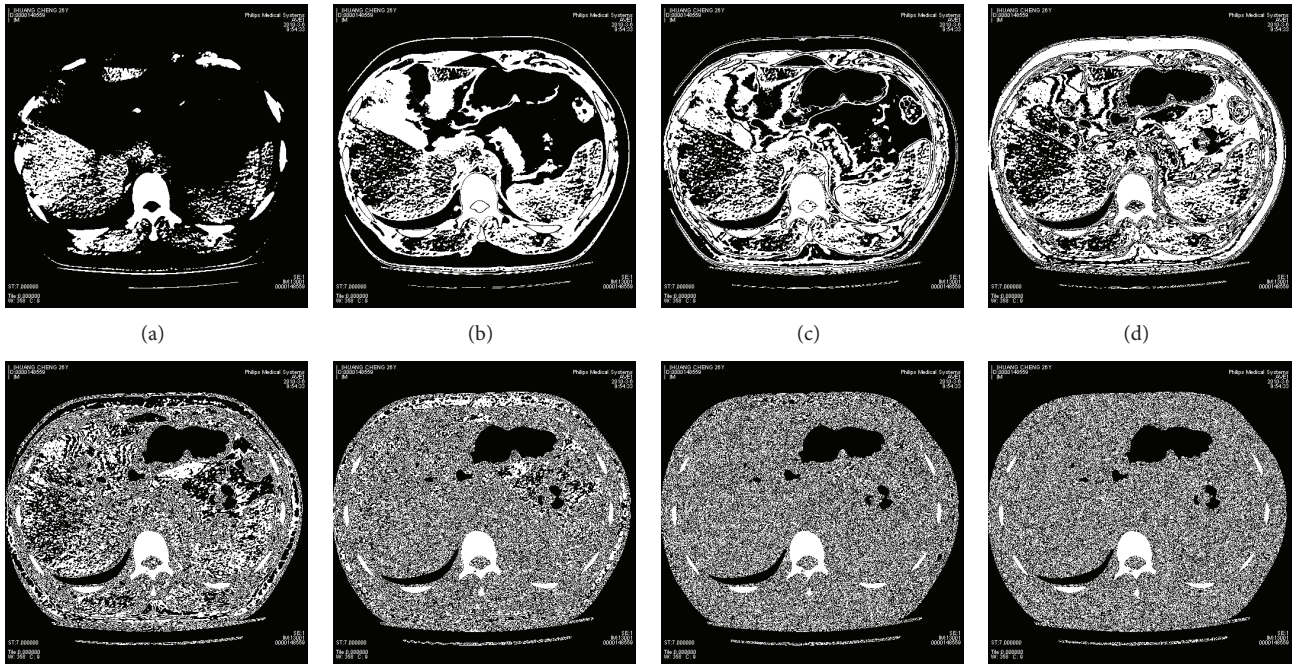


Figure 2: Bit planes of plain image: (a)–(h) are the bit planes from highest bit to the lowest one, respectively.

which will bring about great challenges for the real-time secure medical image transmission. Even for one round encryption of the original scheme, three-round bit-level permutations are also unnecessary; it does little contribution to the security promotion whereas it devotes considerable computational workloads. Detailed analyses and corresponding improvement are both included in this section.

3.1. Cryptanalysis Using Chosen-Plaintext Attack. Firstly, let us recall the achievements proposed in [10]. Wang et al. pointed out that the confusion effect in the cryptosystem under permutation-substitution architecture can be removed if the plain image is with identical pixels. In this case, the security of a cryptosystem solely relies on the substitution procedure. We employ this concept and use a complete black image as the input.

Now, we consider the pixel value modification equation, as defined in (3), and we can get

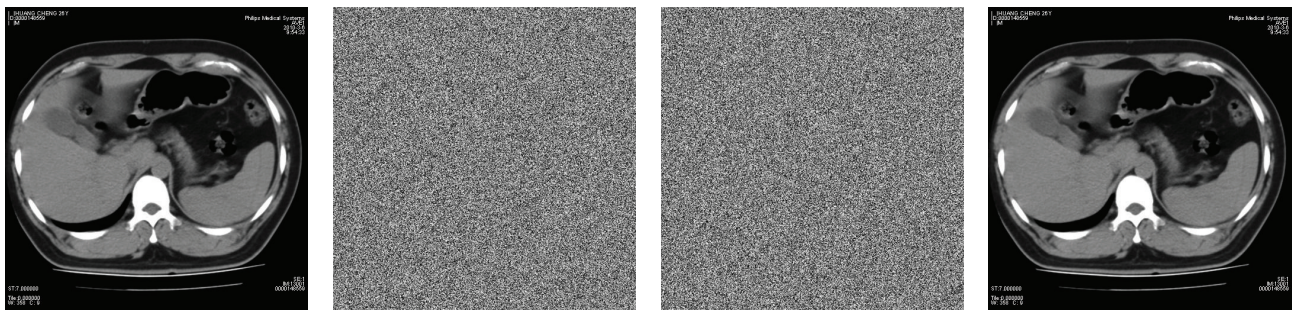
$$k(n) = p(n) \oplus c(n) \oplus c(n-1). \tag{6}$$

When $p(n) = 0$, the above equation can be further simplified to

$$k(n) = c(n) \oplus c(n-1). \tag{7}$$

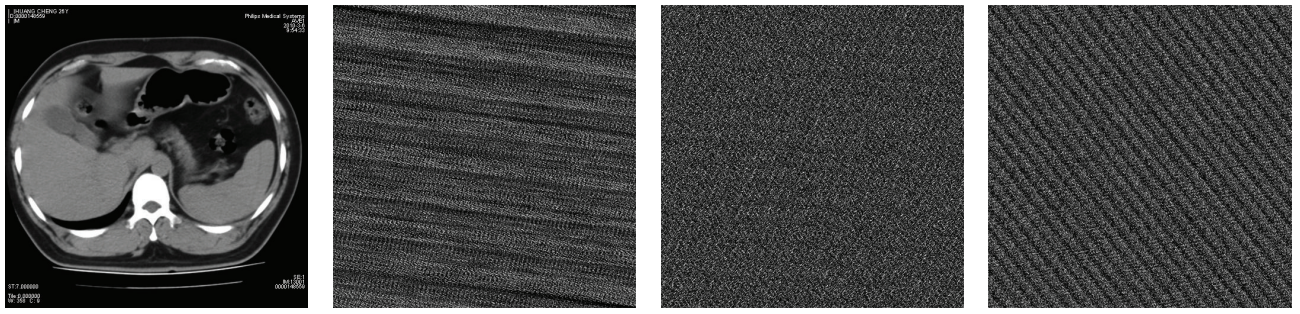
Therefore, the key stream elements in the substitution procedure can be successfully retrieved when using a complete black image as the input.

Once the substitution effects are broken, the resultant image becomes the permutation-only version of the plain image. As described in the previous section, bit-level permutation approach is used in this cryptosystem, with each bit plane shuffling separately with different control parameters. Therefore, we have to recover the permutation matrices for all bit planes. In [31], researchers proposed an optimal



(a) (b) (c) (d)

Figure 3: The results of the proposed chosen-plaintext attack: (a) plain image; (b) cipher image; (c) retrieved substitution key stream elements; (d) the recovered image.



(a) (b) (c) (d)

Figure 4: The resultant images using bit-level permutation: (a) plain image; (b) 1 round permutated image; (c) 3 rounds permutated image; (d) 5 rounds permutated image.

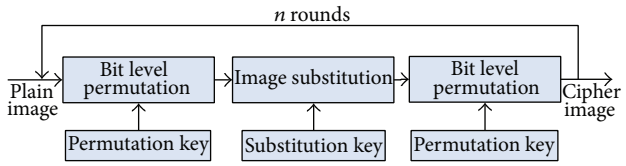


Figure 5: The schematic of the improved cryptosystem.

cryptanalysis of permutation-only multimedia ciphers. The developed method can precisely recover the permutation matrix using several chosen plaintexts. The required number of the chosen plaintexts is given in (8), where M, N, and L represent the width, length, and gray level of the image, respectively. For bit-level permutation case, L is 2. Similar approach can also be found in [24]. In the present paper, we follow the pioneering achievements proposed in [31] to break the bit-level permutation approach of the scheme under study. Eighteen chosen plaintexts are elaborately constructed, and the permutation matrices are all successfully recovered:

$$n = \log_L (M * N). \tag{8}$$

To verify the abovementioned cryptanalysis, we have performed an attack on the encryption scheme. As shown in Figure 3(a), the plain image is a grayscale CT of Abdomen with size 512 × 512, and its corresponding cipher image is demonstrated in Figure 3(b). Figure 3(c) depicts the retrieved key stream elements of the substitution procedure by launching chosen-plaintext attack with a black image, while Figure 3(d) illustrates the final recovered image using the abovementioned chosen-plaintext attacks. The recovered image is consistent with the plain image.

3.2. Improvement of the Medical Image Encryption Scheme

3.2.1. Vulnerability Analysis. In [30], authors declared that certain pixel modification effect can be obtained in the bit-level permutation procedure and such was the case in our simulation. However, let us make microscopic analysis to each of the bit planes. The bit distribution in each bit-plane keeps unchanging after the permutation, as there is no modification of the bit values. When the confused bit planes combine back to an integral image, the pixel values may be changed, but these modifications have no contribution to the security performance. The security contribution of the permutation procedure can also be removed by launching plain images with identical pixel values, in which bit values within the corresponding bit planes are all identical. Once the permutation effect is removed, the security performance solely relies on the substitution procedure, which is generally a kind of pixel masking calculation, as shown in (3). Under chosen/known-plaintext attack, opponents can undoubtedly

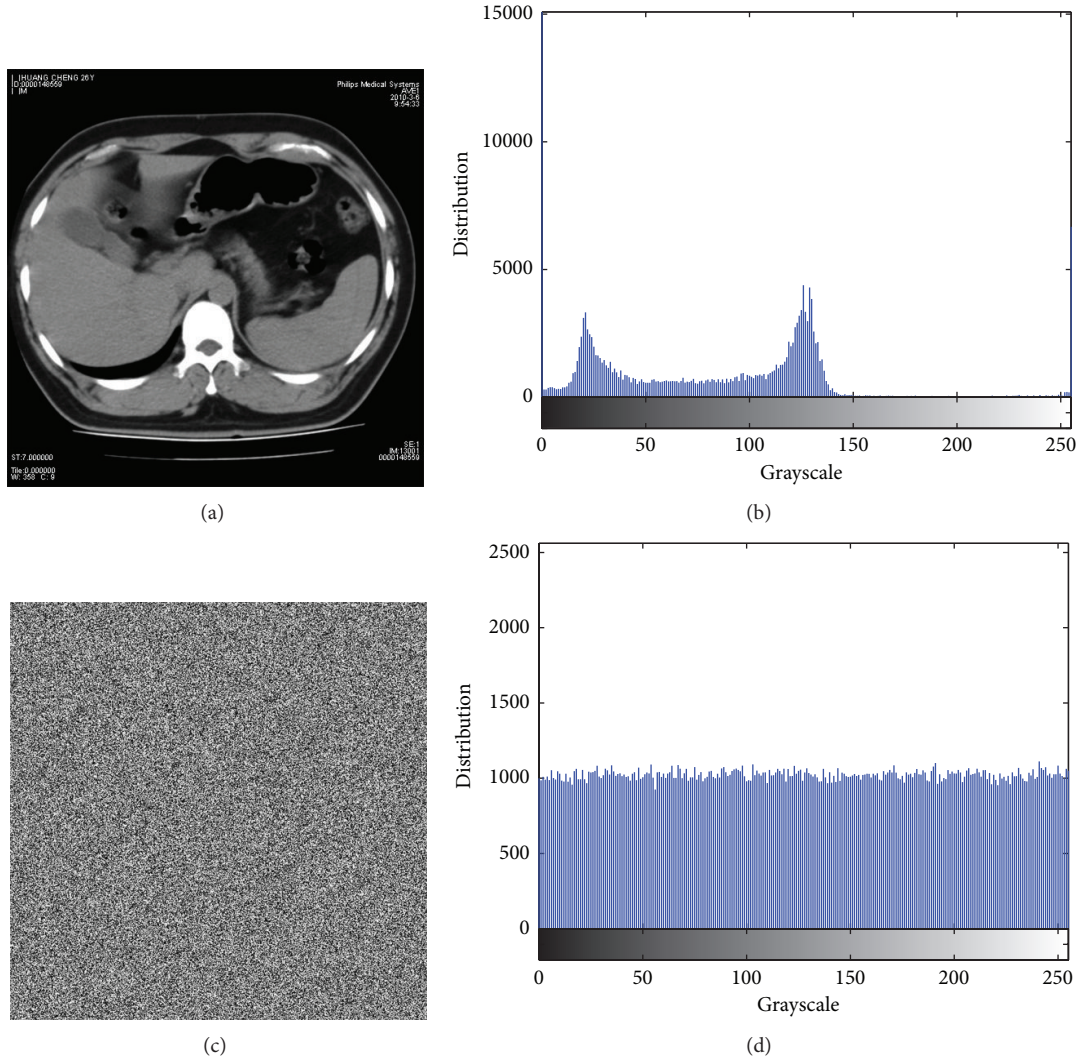


Figure 6: Histogram analysis: (a) plain image; (b) histogram of the plain image; (c) cipher image; (d) histogram of the cipher image.

Table 1: Security contribution of the bit-level permutation in different rounds.

Rounds	Pixel correlation			MSE	Time (ms)
	Horizontal	Vertical	Diagonal		
0 (plain image)	0.9532	0.9301	0.9004	—	—
1	−0.0728	0.0582	−0.0565	7190.2	22
2	0.0805	0.0518	0.0039	7190.8	34
3	0.0416	−0.0428	−0.0427	7191.7	44
5	−0.0498	−0.0479	0.1060	7217.8	68

Table 2: Correlation coefficients of adjacent pixels.

Direction	Plain image	Cipher image
Horizontal	0.9532	0.0035
Vertical	0.9301	$-3.7461e-004$
Diagonal	0.9004	0.0023

retrieve the key stream elements using mathematic deduction, as demonstrated in (6)-(7). After the substitution key stream elements have been recovered, there are various types of methods for the attackers to go back to retrieve the permutation matrix [24, 31], and then the whole cryptosystem is completely broken. The chosen-plaintext attack in the previous section is a successful cryptanalysis of this kind.

However, if we pad an additional (even lightweight) permutation procedure after the substitution process, the

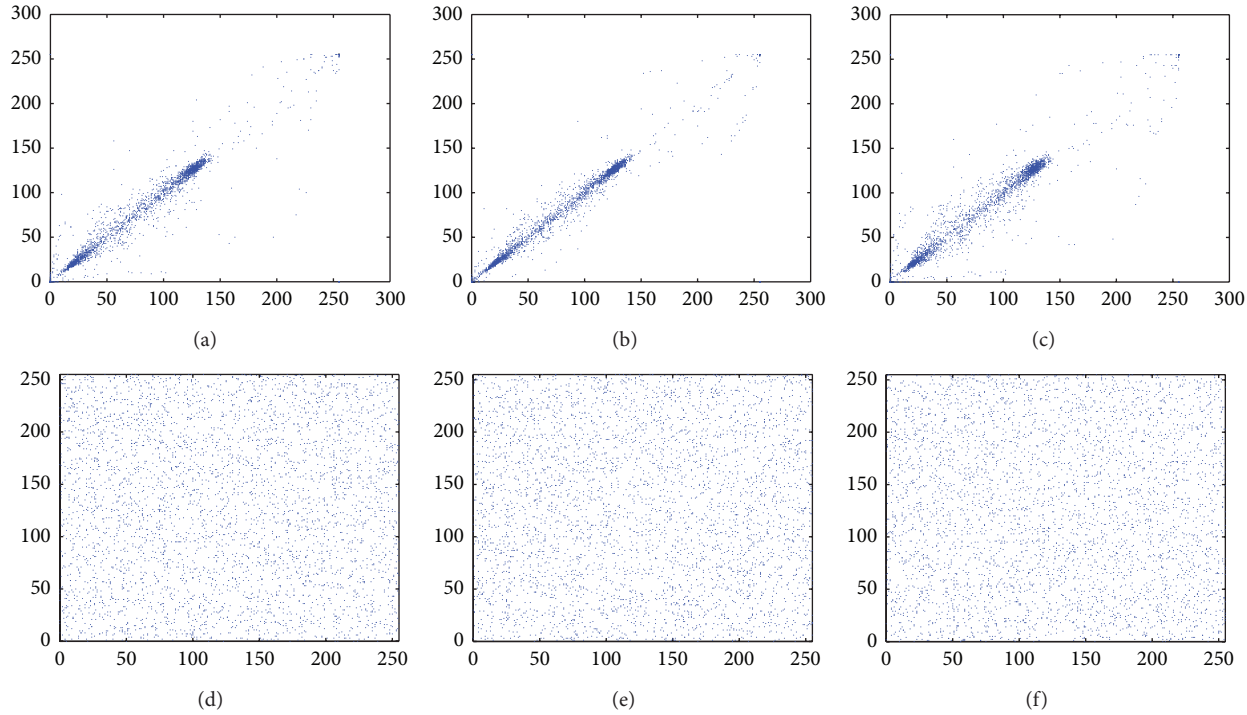


Figure 7: Correlation plots of two adjacent plain image pixels in (a) horizontal, (b) vertical, and (c) diagonal directions; correlation plots of two adjacent pixels of the cipher image in (d) horizontal, (e) vertical, and (f) diagonal directions.

Table 3: Entropies of plain images and cipher images.

	Plain images	Cipher images
CT_Abdomen	5.393012	7.999323
MR_Waist	6.120326	7.999312
X_Lungs	6.966350	7.999353
CT_Paranasal_sinus	3.328586	7.999324
MR_Knee	5.384937	7.999296

security can be significantly enhanced. That is, the cryptosystem is now with permutation-diffusion-permutation architecture. Under this scheme, the plaintext with identical pixels can also effectively remove the confusion effect of the first permutation module. Yet, the pixel values must be masked with chaotic key stream elements in the substitution stage. As the substituted image will be an undoubtedly noise-like one no matter what the plain image is, the confusion effect of the rear-mounted permutation procedure cannot be removed. The substituted image will then be permutated again, and more security is provided. In conclusion, opponents can never remove the image permutation effect no matter what chosen-plaintext attacks are implemented. The plain image will always be protected by both the permutation key and the substitution key.

3.2.2. Efficiency Analysis. Except for the security, the efficiency of the original scheme is also worth discussing. We found that three-round bit-level permutation is redundant. There is little contrition to the security promotion whereas it brings about considerable computational workload. As each of the bit planes is permutated independently with different control parameters, hence actually 24 rounds of bit-level permutation have to be implemented in a single overall encryption round. We have simulated the algorithm by running the standard C program on our platform, a personal computer with an Intel(R) Core(TM) i5 CPU (2.27 GHZ), 2 GB memory, and 320 GB hard-disk capacity, with the compile environment being code blocks 10.05. In our simulation, 62 ms are required for completing one round overall encryption, whereas approximately 44 ms are consumed by the bit-level permutation operations. Besides, the security contribution of the bit-level permutation in different rounds has also been numerically and systematically analyzed.

As described above, permutation in bit level can provide security contribution in two aspects. The first one is the basic image confusion effect, weakening the correlation between adjacent pixels. The correlations of two adjacent pixels in horizontal, vertical, and diagonal directions are calculated according to (9), 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:

$$r_{xy} = \frac{E\left(x - E\left(x\right)\right)\left(y - E\left(y\right)\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}},$$

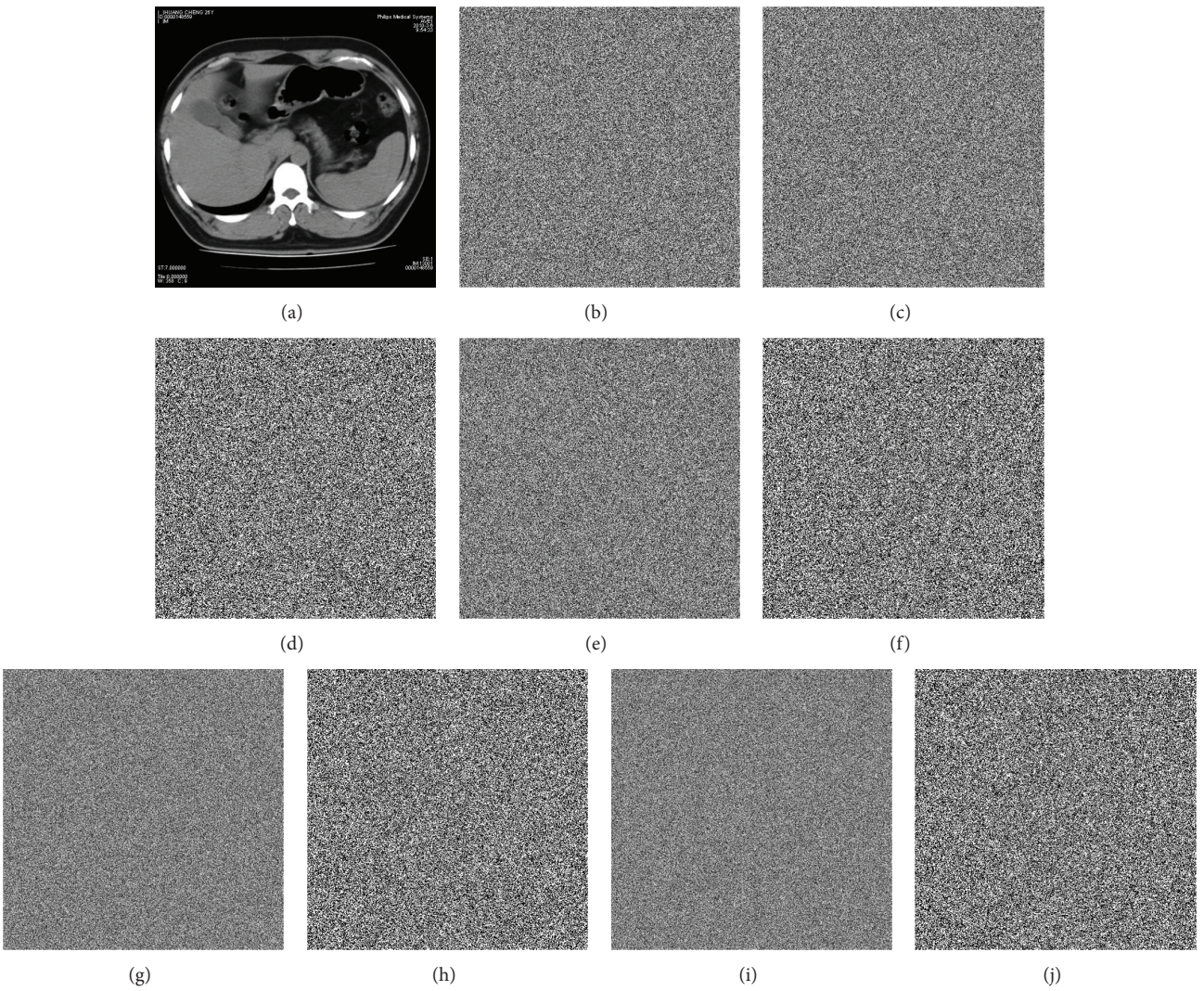


FIGURE 8: Key sensitivity in the first case: (a) plain image; (b) cipher image ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$); (c) cipher image ($p = 41$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$); (d) differential image between (b) and (c); (e) cipher image ($p = 40$, $q = 9$, $x_0 = 0.3$, and $\mu = 3.999$); (f) differential image between (b) and (e); (g) cipher image ($p = 40$, $q = 8$, $x_0 = 0.3 + 10^{-14}$, and $\mu = 3.999$); (h) differential image between (b) and (g); (i) cipher image ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999 + 10^{-14}$); (j) differential image between (b) and (i).

TABLE 4: Differences between cipher images produced by slightly different keys.

Figures	Encryption keys				Differences between Figure 8(b)
	p	q	x_0	μ	
Figure 8(c)	41	8	0.3	3.999	99.60%
Figure 8(e)	40	9	0.3	3.999	99.63%
Figure 8(g)	40	8	$0.3 + 10^{-14}$	3.999	99.61%
Figure 8(i)	40	8	0.3	$3.999 + 10^{-14}$	99.59%

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

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2. \tag{9}$$

The second contribution of bit-level permutation is the pixel value modification effect. The mean square error (MSE) function [17] is introduced to numerically evaluate this performance. The MSE is defined in (10), in which $p_1(m, n)$ and $p_2(m, n)$ denote the plain image and the permutated

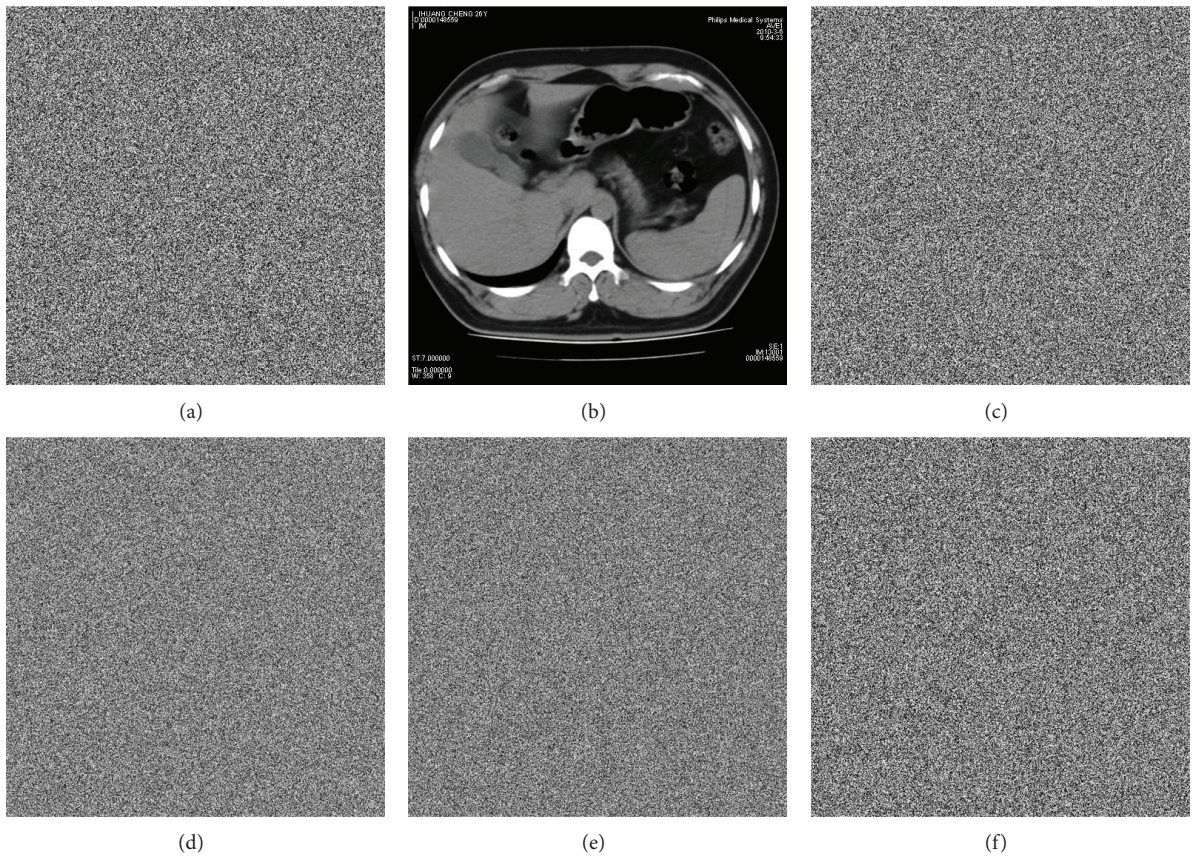


Figure 9: Key sensitivity of the second case: (a) cipher image ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$); (b) decipher image ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$); (c) decipher image ($p = 41$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$); (d) decipher image ($p = 40$, $q = 9$, $x_0 = 0.3$, and $\mu = 3.999$); (e) decipher image ($p = 40$, $q = 8$, $x_0 = 0.3 + 10^{-14}$, and $\mu = 3.999$); (f) decipher image ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999 + 10^{-14}$).

Table 5: Encryption time of the comparable cryptosystems.

Image size	Gray scale	File size	Original scheme (ms)	DES (ms)	Improved scheme (ms)
256 × 256	8-bit	64 K	18.8	51.2	12.6
256 × 256	16-bit	128 K	34.4	86.7	23.2
512 × 512	8-bit	256 K	62.4	206.8	47.8
512 × 512	16-bit	512 K	131.6	414.9	86.2
1024 × 1024	8-bit	1 M	256.7	766.6	170.5
1024 × 1024	16-bit	2 M	504.6	1461.2	328.8

image at coordinates (m, n), respectively, and M and N represent the width and length of the images:

$$\text{MSE} = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} \left| p_1(m,n) - p_2(m,n) \right|^2. \quad (10)$$

The security contribution of the bit-level permutation in different rounds is listed in Table 1, while the resultant images after 1-, 3-, and 5-round bit-level permutation are depicted in Figure 4. The reason why the encryption time of the bit-level permutation dose did not linearly increase has been detailed and analyzed in [30].

As can be seen, the pixel correlation coefficients and pixel modification effect are both stable and satisfactory after one-round bit-level permutation; meanwhile, all of the resultant images are unrecognizable. It convincingly proves that a satisfactory security performance can be obtained in the first round bit-level permutation, whereas more times permutation cannot provide distinct security promotion. To sum up, only one-round bit-level permutation is essentially required in this cryptosystem.

3.2.3. The Improved Scheme. On the basis of the abovementioned achievements, we improve the original cryptosystem. The improved image encryption scheme is shown in Figure 5. In a single overall round, one-round bit-level permutation is performed firstly, and then the permutated image enters

into the image substitution procedure. At last, the resultant image after the substitution phase will be permutated again to enhance the security. The abovementioned processes can be performed many times to satisfy the security requirements.

The detailed process of the improved cryptosystem is described as follows.

Step 1. Perform one-round bit-level permutation.

(1) Decompose the plain image into bit planes.

(2) Shuffle each bit plane with separate control parameters.

(3) Combine all the shuffled bit planes together to produce the permutated image.

Step 2. Perform one-round image substitution.

(4) Iterate (5) with (x_0, μ) for N_0 times continuously to avoid the harmful effect of transitional procedure, where N_0 is a constant.

(5) Iterate the chaotic map once and get the key stream elements for current substitution according to (4).

(6) Calculate the cipher pixel value according to (3). For the first pixel, initial value $c(-1)$ has to be set as a seed.

(7) Go back to (5) until all pixels are encrypted.

Step 3. Perform one-round bit-level permutation.

(8) Decompose the plain image into bit planes.

(9) Shuffle each bit plane with separate control parameters.

(10) Combine all the shuffled bit planes together to produce the cipher image.

Step 4. Repeat the abovementioned steps n times to satisfy the security requirements.

In the improved scheme, the parameters of cat map, p and q, the control parameters of logistic map, x_0 and μ jointly compose the secret key.

The decryption procedure is similar to that of the encryption process illustrated above, with the reverse operational sequences. As both decryption and encryption procedures are with similar architectures, they have essentially the same algorithmic complexity and time consumption.

4. Security Analyses

In this section, extensive security analyses are carried out to evaluate the security performance of the improved scheme. The security indices consist of various statistical analyses, key space analysis, key sensitivity test, and encryption speed. Except for the encryption speed, other performances are basic cryptography indices. There is no notable performance difference for effective encryption algorithms, and hence we do not make comparisons in terms of these indices, as described in Sections 4.1–4.3. The resistance to known-/chosen-plaintext attack of the improved scheme has been reported in the previous section. We will describe the speed performance promotion of the improved scheme in detail in Section 4.4, in comparison with the original scheme and the well-known DES. Consistent with the original paper, the encrypted image after two overall rounds is adopted.

4.1. Statistical Analysis

4.1.1. Histogram Analysis. Histogram of a digital image shows the distribution information of the pixel values. An effective image cryptosystem should produce ciphertext with uniform histogram. The histograms of the plain image and its corresponding cipher image produced by the improved cryptosystem are shown in Figures 6(b) and 6(d), respectively. It is obvious that the histogram of the encrypted image is uniformly distributed and quite different from that of the plain image, which implies that the redundancy of the plain image is successfully hidden after the encryption and consequently does not provide any clue to apply statistical attacks.

4.1.2. Correlation of Adjacent Pixels. For an ordinary image with meaningful visual perception, the correlation between adjacent pixels is always high as their pixel values are close to each other. An effective image cryptosystem should make sure that the cipher images are 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 (9). The correlation coefficients of adjacent pixels in the plain image and its cipher image are listed in Table 2. Moreover, the correlation of the adjacent pixels in the plain and the encrypted image are depicted in Figure 7. Both the calculated correlation coefficients and the figures can substantiate that the strong correlation among neighboring pixels of the plain image can be effectively decorrelated by the proposed cryptosystem.

4.1.3. Information Entropy. Information entropy is a mathematical property that reflects the randomness and the unpredictability of an information source that is first found in 1949 by Shannon [32]. The entropy $H(s)$ of a message source s is defined as

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i) \log_2 P(s_i), \tag{11}$$

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, the entropy of a cipher image with 256 gray levels should ideally be 8. Otherwise, the information source is not sufficiently random and there exists a certain degree of predictability, which threatens its security.

Five 256 gray-scale medical images with size 512×512 are encrypted and the information entropies are then calculated, as 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 information leakage in the encryption procedure is negligible and the proposed algorithm is secure against entropy analysis.

4.2. Key Space Analysis. The key space size is the set of all possible keys that can be used in a cryptosystem. In [29], Alvarez and Li suggested that the key space should be at least 2^{100} for a sufficient security level making the brute force attack infeasible. The key of the proposed cryptosystem is composed of two parts, permutation key Key_p and substitution key Key_s. The initial value x_0 and the control parameter μ of the logistic map serve as the substitution key, where $x_0 \in [0, 1]$ and $\mu \in [3.57, 4]$. According to the IEEE floating-point standard [33], the computational precision of the 64-bit double-precision number is about 10^{-15}, and hence the total numbers of possible values of x_0 and μ are approximately 10^{15} and 0.43×10^{15}, respectively. For discretized cat map, the size of secret key is $(N^2)^m$, where N is the image size and m is the iteration times. Therefore the Key_p of the improved scheme is N^2. As the two parts Key_p and Key_s are independent of each other, hence the total key space of the proposed cryptosystem is

$$\text{Key}_{\text{total}} = \text{Key}_p \times \text{Key}_s \approx N^2 \times 0.43 \times 10^{15} \times 10^{15}. \quad (12)$$

If $N \geq 256$, the total size is

$$\text{Key}_{\text{total}}(p, q, \mu, x_0) \geq 2^{114}, \quad (13)$$

which satisfies the key space requirements suggested in [29], and is sufficiently large to resist brute attack.

4.3. Key Sensitivity Test. Extreme key sensitivity is a crucial feature of an effective cryptosystem and can be evaluated in two aspects: (1) completely different cipher images should be produced when the plain image is encrypted with slightly different secret keys; (2) the cipher image cannot be correctly decrypted even if slight difference exists between the encryption and decryption keys.

To evaluate the key sensitivity in the first case, the encryption is firstly carried out to obtain a cipher image with coefficients ($p = 40$, $q = 8$, $x_0 = 0.3$, and $\mu = 3.999$). Then a slight change is introduced to one of the parameters with all others keeping the same and then repeating the encryption process. The corresponding cipher images and the differential images are shown in Figure 8. The differences between the corresponding cipher images are calculated and given out in Table 4. The results obviously demonstrate that the cipher images exhibit no similarity to one another and there is no significant correlation that could be observed from the differential images.

In addition, decryption using keys with slight changes as described above is also performed so as to evaluate the key sensitivity of the second case. The decipher images are shown in Figure 9. The differences between wrong decipher images (Figures 9(c), 9(d), 9(e), and 9(f)) to the plain image (Figure 9(b)) are 99.60%, 99.59%, 99.59%, and 99.61%, respectively.

The above two tests indicate that the proposed image encryption scheme is highly sensitive to the key. Even an almost perfect guess of the key does not reveal any valuable information about the cryptosystem and hence differential attack would become inefficient and practically useless.

4.4. Speed Performance. Once the security requirement is fulfilled, the operation speed becomes an essential factor for real-time teleradiology applications. The encryption speed of the improved scheme is evaluated and compared with the original cryptosystem and the well-known DES technique, using medical images with various sizes. The speed is measured by running the standard C program on our simulation platform as described before. The results are listed in Table 5.

According to the comparative experimental results, the improved scheme has more satisfactory encryption efficiency than the original one. The promotion of the encryption speed is obtained by reducing the counts of bit-level permutation operations, which is the highest cost of the original scheme. In comparison with DES, the speed superiority is more obvious. The improved scheme is appropriate for the applications in real-time teleradiology and other telehealth cares where the encryption time should be short relatively to the transmission time.

5. Conclusions

In this paper, we give out detailed analyses of an efficient and secure medical image protection scheme proposed recently. Cryptanalysis and experimental results both prove the vulnerability to chosen-plaintext attacks of that scheme. The corresponding improvement to enhance the security performance is subsequently proposed. Security analyses and simulation results have proved the higher security level and efficiency of the proposed scheme, which is a good candidate for real-time teleradiology applications.

Conflict of Interests

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

Acknowledgments

This work was supported by Programs for Science and Technology Development of LiaoNing Province (no. 20132250361-13, research on regional collaborative medical imaging information platform; no. 2013225089, research on imaging of children's congenital heart disease using multislice CT).

References

[1] J. Hu and F. Han, "A pixel-based scrambling scheme for digital medical images protection," *Journal of Network and Computer Applications*, vol. 32, no. 4, pp. 788–794, 2009.

[2] J. Montagnat, F. Bellet, H. Benoit-Cattin et al., "Medical images simulation, storage, and processing on the European Data Grid

testbed," *Journal of Grid Computing*, vol. 2, no. 4, pp. 387–400, 2004.

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

[4] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics*, vol. 29, no. 5, pp. 367–383, 2005.

[5] 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.

[6] 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/hipaa/administrative/index.html.

[7] HEMA, DICOM: digital imaging and communication in medicine, http://medical.nema.org/.

[8] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, chapter 4, pp. 133–167, CRC Press, New York, NY, USA, 2005.

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

[10] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[11] Y. Zhang, D. Xiao, H. Liu, and H. Nan, "GLS coding based security solution to JPEG with the structure of aggregated compression and encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 5, pp. 1366–1374, 2014.

[12] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[13] 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.

[14] 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.

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

[16] J. Chen, Z. ZHu, L. Zhang, C. Fu, and H. Yu, "An efficient diffusion scheme for chaos-based digital image encryption," *Mathematical Problems in Engineering*, vol. 2014, Article ID 427349, 13 pages, 2014.

[17] J.-X. Chen, Z.-L. Zhu, Z. Liu, C. Fu, L.-B. Zhang, and H. Yu, "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," *Optics Express*, vol. 22, no. 6, pp. 7349–7361, 2014.

[18] 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.

[19] 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.

[20] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Applied Soft Computing Journal*, vol. 11, no. 1, pp. 514–522, 2011.

[21] X. Y. Zhang, C. Wang, S. Zhong, and Q. Yao, "Image encryption scheme based on balanced two-dimensional cellular automata," *Mathematical Problems in Engineering*, vol. 2013, Article ID 562768, 10 pages, 2013.

[22] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters A*, vol. 343, no. 6, pp. 432–439, 2005.

[23] Y. Zhang, W. Wen, M. Su, and M. Li, "Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Optik*, vol. 125, no. 4, pp. 1562–1564, 2014.

[24] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K.-T. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication*, vol. 23, no. 3, pp. 212–223, 2008.

[25] X. Wang and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 24, pp. 5404–5407, 2011.

[26] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dynamics*, vol. 76, no. 3, pp. 1645–1650, 2014.

[27] C. Zhu, C. Liao, and X. Deng, "Breaking and improving an image encryption scheme based on total shuffling scheme," *Nonlinear Dynamics*, vol. 71, no. 1-2, pp. 25–34, 2013.

[28] J. X. Chen, Z. L. Zhu, C. Fu, L. B. Zhang, and Y. Zhang, "Cryptanalysis and improvement of an optical image encryption scheme using chaotic Baker map and double random phase encoding," *Journal of Optics*, vol. 16, no. 2, Article ID 125403, 13 pages, 2014.

[29] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 16, no. 8, pp. 2129–2151, 2006.

[30] 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.

[31] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing*, vol. 91, no. 4, pp. 949–954, 2011.

[32] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[33] IEEE Computer Society, *IEEE Standard for Binary Floating-Point Arithmetic*, ANSI/IEEE, 1985.