International Journal of Signal Processing, Image Processing and Pattern Recognition
Vol.8, No.7 (2015), pp.327-340
http://dx.doi.org/10.14257/ijsip.2015.8.7.32

An Efficient Cryptosystem for Medical Image Encryption

Li-bo Zhang[1,2] and Ben-qiang Yang[2,*]

[1]*Software College, Northeastern University, No. 11, Lane 3, WenHua Road, Shenyang 110004, China*
[2]*Department of radiology, General Hospital of Shenyang Military Area Command, No. 83, Wenhua Road, Shenyang, 110004, China*
zhanglibo.neu@gmail.com, benqiang.y@gmail.com

Abstract

Nowadays, the increasing requirement for telemedicine services has raised more concerns in real-time medical image encryption. However, traditional block ciphers have been found poorly fit this requirement. Considering this, we propose an efficient cryptosystem for medical image encryption in the present study. Chaos-based permutation-diffusion architecture is adopted, whereas an improved image confusion strategy is developed based on the intrinsic feature of medical images. The improved confusion approach can bring about not only satisfactory permutation performance but also bit distribution balancing effect for medical images. Simulations and extensive security analyses indicate that the proposed cryptosystem provides an efficient approach for real-time secure medical image transmission and storage over public networks.

Keywords: *medical image encryption, chaos, improved confusion, standard map*

1. Introduction

With the rapid development of networking and communication technologies, medical images have act as important roles in the field of telediagnosis, telesurgery and so on [1-4]. As medical images are private and confidential data of patients, the security of their storage and transmission over public networks has become an important issue. Mandates guidelines, such as Health Insurance Portability and Accountability Act (HIPAA) [5-6], Picture Archiving and Communication Systems (PACS) as well as Digital Imaging and Communications in Medicine (DICOM) standard, continue to be published by organizations focus on healthcare [7]. However, PACS is designed for archiving and distributing medical image data within an internal hospital network that is usually protected by a firewall against outside intruders. If the communication extends over public networks, it may leave thousands of opportunities for an intruder, casual or with malicious intent, to tamper the private data over open networks [6]. Security of medical images storage and transmission over public networks faces tremendous threats.

Encryption is the most convenient way for data protection. However, traditional block ciphers such as DES, Triple-DES and AES that are originally designed for encrypting textual data have been found poorly suitable for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [8]. Meanwhile, many researchers have noticed that the fundamental features of chaotic systems such as ergodicity, mixing property, unpredictability, sensitivity to initial conditions/system parameters, et al. can be considered analogous to some ideal cryptographic properties for image encryption. In [9], Fridrich first proposed general permutation-diffusion architecture for chaos-based image cryptosystem. Under this structure, a plain image is firstly shuffled by a two-dimensional area-preserving chaotic map so as to erase the high correlation between

ISSN: 2005-4254 IJSIP

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 consequently proposed [10-25]. Recently, chaos-based cryptosystems have also been employed for medical applications [26-27]. In [26], a chaos-based visual encryption mechanism for clinical electroencephalography signals is developed, whereas a medical image protection scheme is built in [27].

In this paper, we proposed an efficient medical image encryption scheme. The typical permutation-diffusion architecture is adopted, whereas an improved permutation strategy is investigated. The new confusion approach is developed on the basis of the intrinsic features of medical images, and can significantly accelerate the encryption efficiency for medical images. Collaborating with an image diffusion procedure, a complete cryptosystem is built. Simulations and security analyses well demonstrate the security of this cryptosystem. The remainder of this paper is organized as follows. In the next section, we briefly review the typical architecture of chaos-based image encryption scheme. The proposed cryptosystem for medical image encryption will be presented in detail in Section 3. Simulations and extensive security analyses are carried out in Section 4. Finally, conclusions will be drawn in the last section.

2. Permutation-diffusion Architecture

The architecture of typical chaos-based image cryptosystems is sketched in Figure 1. There are two stages in the cryptosystems of this type, the so-called permutation stage and diffusion stage.

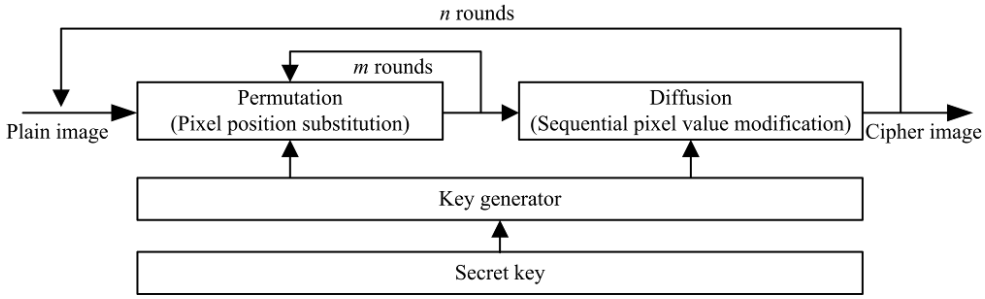


Figure 1. Architecture of Typical Chaos-based Image Cryptosystems

In the permutation stage, pixels in the plain image are usually shuffled by a kind of two-dimensional area-preserving chaotic map. Three types of maps, Arnold cat map, standard map and baker map are usually employed and their discretized versions are given by Eqs. (1)-(3), respectively. In these equations, N represents the width or height of the square image, (x_i, y_i) and (x_{i+1}, y_{i+1}) are the original and the permuted pixel positions, (p, q), n_j (j=1, 2, … , t-1) and K are control parameters of the three maps, respectively. All pixels are generally shuffled sequentially from upper-left corner to lower-right corner, and then the permutated image is produced.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{1}$$

$$\begin{cases} x_{i+1} = (x_i + y_i) \bmod N \\ y_{i+1} = (y_i + K \sin \dfrac{x_{i+1} N}{2\pi}) \bmod N \end{cases}, \tag{2}$$

$$\begin{cases} x_{i+1} = \dfrac{N}{n_j}(x_i - N_j) + y_i \bmod \dfrac{N}{n_j} \\ y_{i+1} = \dfrac{k_j}{N}(y_i - y_i \bmod \dfrac{N}{n_j}) + N_j \end{cases}, \ where \begin{cases} n_0 + n_1 + \cdots + n_t = N \\ N_j = n_0 + n_1 + \cdots + n_j \\ 0 \le y_i \le N \\ N_j \le x_i \le N_j + n_{j+1} \\ 0 \le j \le t-1 \\ n_0 = 0 \end{cases}. \quad (3)$$

In the diffusion procedure, pixel values are modified sequentially by mixing with the key stream elements that are generated by a one-dimensional chaotic map. Generally, the modification of a particular pixel not only depends on the corresponding key stream element but also the accumulated effect of the previous pixel values. A typical diffusion operation is illustrated in Eq. (4), where $p(n)$, $k(n)$, $c(n)$, and $c(n\text{-}1)$ represent the current plain pixel, key stream element, output cipher-pixel and the previous cipher-pixel, respectively.

$$c(n) = k(n) \oplus p(n) \oplus c(n-1). \quad (4)$$

Such diffusion approach can spread a slight change of the plain image to a large scale in the cipher image and thus differential attack may be practically useless. Additionally, to cipher the first pixel, $c(\text{-}1)$ has to be set as a seed.

3. The Proposed Medical Image Cryptosystem

3.1. Bit Distributions of Medical Images

Unlike traditional pixel-level analysis of images, a 256 gray levels image can also be regarded as a 3-D binary matrix using Eq. (5), and then the image is a set of bit values.

$$B(i,m,n) = \{b_{mn}^i \,|\, m \in [0, M-1], n \in [0, N-1], i = 1,2,3...,8\}. \quad (5)$$

In this equation, M and N represents the width and length of the image, and b_{mn}^i is the bit value with coordinates (m, n) in the ith bit plane [30]. According to the previous achievements in [30], the count of '0' and '1' of a natural image always follow the uniform distribution. In other words, the percentage of '0' and '1' is almost the same with each other, each of them is close to 50%. However, we found that this achievement does not hold for medical images, in which the percentage of '0' is much greater than that of '1'. Sixteen medical images and natural images of size 512×512 are employed for verification. The introduced eight natural images are shown in Figure 2, all of which are downloaded from the USC-SIPI image database, available at http://sipi.usc.edu/database/. The employed medical images are depicted in Figure 3. As observed from the caption of Figure 3, the medical images are named after classification_organ. For example, CT_Abdomen represents a CT image of Abdomen. The percentage of '0' and '1' of the natural images is listed in Table 1, whereas the bit distribution of medical images is listed in Table 2.

It is obvious shown that the percentage of '0' is much greater than that of '1' in medical images, much different with that of the natural images. This property can also be visually revealed from the perception that medical images are always darker than natural images. As we know, image permutation is applied to shuffle the pixels at pixel-level or bit-level without any modification to their values. Therefore, the resultant image after any rounds permutation will always be very dark, as the bit '0' occupies a much larger part in the confused image. The bit modification pressure remains after the permutation stage. How to rapidly balance the '0' and '1' in the medical images is an important factor for accelerating the encryption process.

Figure 2. The Natural Images: (a) Aerial; (b) Airfield; (c) Baboon; (d) Barb; (e) Boats; (f) Bridge; (g) Lena; (h) Peppers

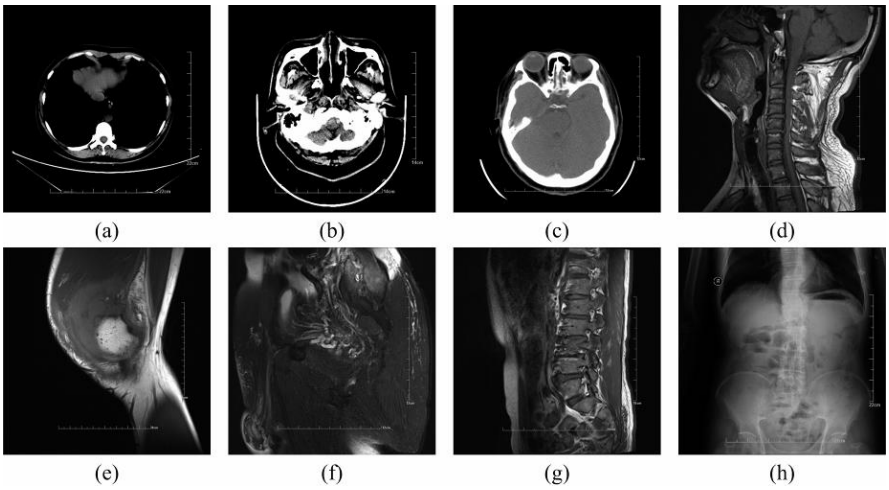


Figure 3. The Medical Test Images: (a) CT_Abdomen; (b) CT_Head; (c) CT_Paranasal_sinus; (d) MR_Cervical_vertebra; (e) MR_Knee; (f) MR_Prostate; (g) MR_Waist; (h) X_Lungs

Table 1. Bit Value Distribution of Natural Images

Test image	Percentage of 0 (%)	Percentage of 1 (%)
Aerial	46.88587189	53.11412811
Airfield	49.14751053	50.85248947
Couple	50.88362694	49.11637306
Dollar	48.22745323	51.77254677
House	50.46553612	49.53446388
Lenna	50.76069832	49.23930168
Monarch	52.95000076	47.04999924
Truck	51.67765617	48.32234383
Average	50.12479425	49.87520576

Table 2. Bit Value Distribution of Medical Images

Test image	Percentage of 0 (%)	Percentage of 1 (%)
CT_Abdomen	93.51091385	6.489086151
CT_Head	82.92846680	17.07153320
CT_Paranasal-sinus	80.32541275	19.67458725
MR_Cervical-vertebra	62.77995110	37.22004890
MR_Knee	68.10107231	31.89892769
MR_Prostate	60.31408310	39.68591690
MR_Waist	63.57970238	36.42029762
X_Lungs	62.84770966	37.15229034
Average	71.79841399	28.20158601

Once the abovementioned concepts are accepted, a feasible approach to promote the efficiency of medical image encryption is therefore generated. That is trying to introduce bit balancing performance and hence pixel value modification effect in the permutation procedure, while simultaneously maintaining a satisfactory image confusion performance. In this scenario, the workload of the time consuming diffusion part is consequently reduced so that fewer encryption rounds and shorter operation time are required.

3.2. Improved Standard Map based Image Permutation

In this section, we will give out a novel image permutation approach as expected above. The improvement can collaborate with any image permutation techniques, and we use standard map as an example for clear illustration. In the improved approach, lightweight and efficient pixel value modification is carried out at the same time with the pixel position permutation operation. Firstly, the shuffled position of a plain pixel is also calculated using standard map, as shown in Eq. (3). However, before the pixel relocation, we will implement a cyclic shift to the plain pixel according to the last four bits of the previous permutated pixel. Then an exclusive OR operation will be implemented between the resultant pixel and the previous permutated pixel to further modify the pixel value. To sum up, the new pixel value that will be moved to the shuffled poison can be demonstrated in Eq. (6), where C_i and $C_{i\text{-}1}$ represent the current and the previous processing pixel value in the permutated image, and P_i is the current plain pixel value. The function $Cyc[s, d, q]$ is the q-bit cyclic shift on the binary sequence s. The cyclic shift in right direction will be implemented if d=1, whereas cyclic shift in left direction will be performed when d=0. The expression $B_4(C_{i\text{-}1})$ is the bit value in the fourth bit position of $C_{i\text{-}1}$, while $LSB_3(C_{i\text{-}1})$ refers to the value of the least three significant bits of $C_{i\text{-}1}$.

$$C_i = Cyc[P_i,\ B_4(C_{i-1}),\ LSB_3(C_{i-1})] \oplus C_{i-1}. \quad (6)$$

Amounts of simulations have been implemented to verify the effectiveness of this improved confusion scheme in terms of pixel correlation performance as well as bit balancing effect. Firstly, we evaluate the pixel correlation performance of the proposed confusion scheme. The CT_Abdomen image shown in figure 3(a), is introduced. Figures 4(a), 4(b), 4(c) and 4(d) represent the permutated images using 1 round standard map, 3 rounds standard map, 5 rounds standard map and 1 round the improved permutation approach, respectively. The pixel correlation coefficients of these confused images are listed in Table 3. From the numerical results, one come to the conclusion that only one round improved image confusion approach is sufficient to achieve a satisfactory pixel correlation performance. The pixel correlation coefficient after using one round improved confusion is better than that of 3 rounds standard map, and the consumption time is also satisfactory. As shown in figure 4(d), the resultant image of the improved confusion approach is completely unrecognizable. Both the figures and the numerical coefficients

prove the pixel correlation performance and the operation efficiency of the proposed confusion approach.

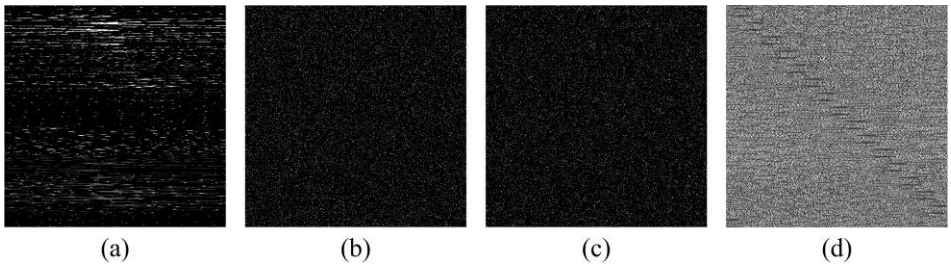


Figure 4. Permutation Effect of the Improved Confusion Approach: Confused with Standard Map 1 Round (a); 2 Rounds (b); 3 Rounds (c); (d) Confused Image with 1 Round the Improved Confusion Approach

Table 3. Pixel Correlation Coefficients of Different Permutation Techniques

Permutation Approach	Rounds	Pixel correlation			Time (ms)
		Horizontal	Vertical	Diagonal	
Plain-image		0.8961	0.9535	0.8780	—
Proposed	1	-0.0069	0.1678	0.0310	32
Standard map	1	0.1320	0.9116	0.1221	30
Standard map	3	0.0124	0.0238	0.0354	90
Standard map	5	-0.0097	0.0168	0.0269	150

As mentioned before, pixel values of the plain image do not change when using traditional permutation techniques, and hence the histograms of the shuffled images produced by any rounds of standard map are the same as that of the plain image. Such is the case in our simulations, as shown in Figure 5. On the contrary, as lightweight pixel value modifications are performed in our strategy, the histogram of the resultant image is different from that of the plain image, and is much more uniform than it, as revealed in Figure 5(c). This property indicates the pixel modification effect of the improved confusion approach.

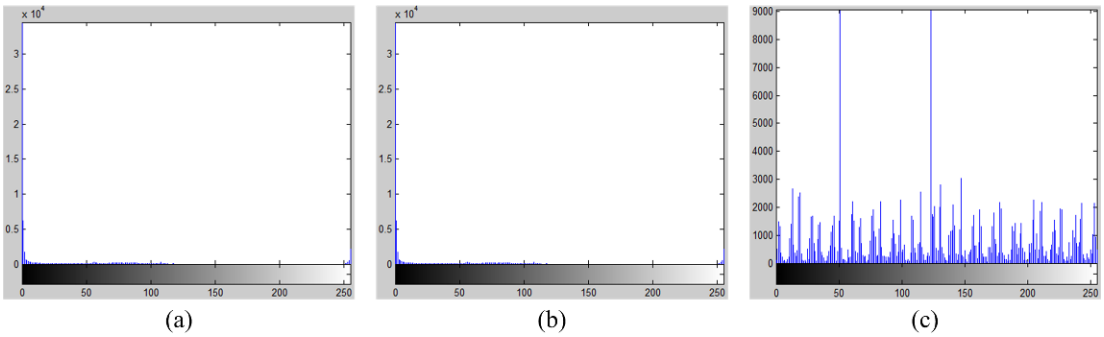


Figure 5. Histograms of the Confused Images using Different Confusion Approaches: (a) Histogram of the Plain Image; (b) Histogram of the Confused Image with 3 Rounds Baker Map; (c) Histogram of the Confused Image with 1 Round the Proposed Confusion Approach

Here, we will demonstrate the bit balancing property of the improved confusion strategy. The bit distribution of 1 and 0 of the permutated medical images after 1 round

improved confusion is listed in Table 4. It can be seen that, after 1 round improved confusion, the pixel values have been lightweight modified, and the bit distribution has also been more balanced. The percentage of 0 or 1 is approximately the same with each other, and is nearly 50%. This property is a basic feature for an effective ciphertext.

Table 4. Bit Value Distribution of the Permutated Medical images

Test image	Percentage of 0 (%)	Percentage of 1 (%)
CT_Abdomen	43.90521049	56.09478951
CT_Head	45.74508667	54.25491333
CT_Paranasal-sinus	45.21799088	54.78200912
MR_Cervical-vertebra	49.84459877	50.15540123
MR_Knee	49.62911606	50.37088394
MR_Prostate	48.78344536	51.21655464
MR_Waist	48.50859642	51.49140358
X_Lungs	49.45354462	50.54645538
Average	47.63594866	52.36405134

3.3. The Complete Medical Image Cryptosystem

The complete cryptosystem is based on permutation-diffusion architecture, with the improved confusion strategy as a replacement of traditional permutation maps, whereas the diffusion keeps the same. When using typical permutation techniques, 3-5 round permutation operations are usually required to achieve a satisfactory image confusion effect. However, only one round improved image confusion approach is required in our scheme. In the diffusion stage, pixel values are modified sequentially according to Eq. (4), and the key stream element $k(n)$ is calculated by Eq. (7), in which $floor(x)$ returns the value nearest integers less than or equal to x, mod(x, y) returns the remainder after division, $x(n)$ is the current state of a chaotic map, and L is the gray level of the plain image, respectively.

$$k(n) = \mathrm{mod}\ [\ floor(x(n) \times 10^{14}),\ L]\ . \tag{7}$$

Chaotic Chebyshev map is employed for key stream generation in the proposed cryptosystem, as described by

$$x_{n+1} = \cos(k \cdot \cos^{-1} x_n), x_n \in [-1,1], \tag{8}$$

where $k \in [2, \infty)$ is the control parameter. The initial value x_0 and the control parameter k are used as the key.

The architecture of the cryptosystem is depicted in figure 6, and the operation procedures are described as follows.

Step 1: Perform one round improved image permutation operation.

(1) Calculate the shuffled position of current plain pixel using cat map, as shown in Eq. (2).
(2) Perform lightweight pixel value modification according to Eq. (6), initial value $c(-1)$ has to be set as a seed for the first pixel.
(3) Write the resultant pixel into the shuffled position of the permutated image.
(4) Go back to (1) until all pixels are permutated.
(5) **Step 2**: Perform one round image diffusion.
(6) Iterate Eq. (8) with (x_0, k) for N_0 times continuously to avoid the harmful effect of transitional procedure, where N_0 is a constant.
(7) Iterate the chaotic map once, and get the key stream elements for current diffusion operation according to Eq. (7).
(8) Calculate the cipher pixel value according to Eq. (4). For the first pixel, initial value $c(-1)$ has to be set as a seed.

(9) Go back to (6) until all pixels are encrypted.

Step 3: Repeat the above steps *n* times to satisfy the security requirements.

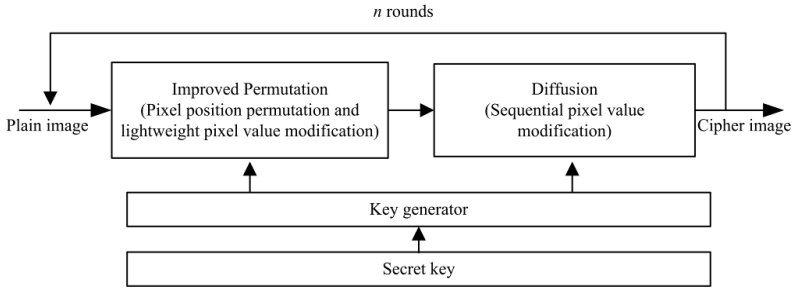


Figure 6. Architecture of the Proposed Cryptosystem

In the proposed cryptosystem, the control parameters of standard map *K*, the initial value x_0 and the control parameter *k* of Chebyshev map jointly compose the secret key.

4. Security Analyses

Amount of simulations have been implemented with different plain images and numbers of encryption rounds to verify the security of the proposed scheme. The cryptosystem is simulated by running standard C program on our computing platform, a personal computer with a Pentium(R) CPU (1.19GHZ), 2GB memory and 320GB hard-disk capacity. The compile environment is Code Blocks 10.05. The secret key is randomly selected as (K=512) for standard map and (k=9.87654321, x_0=0.123456789) for Chebyshev map. The medical images with size 512×512 are employed, while cipher images after 2 rounds encryption are adopted for various security analyses.

4.1. Key Space Analysis

The key space size is the total number of different keys that can be used in a cryptosystem. In [31], researchers suggested that the key space should be at least 2^{100} to resist against the eavesdropping by brute-force attack. The key of the proposed cryptosystem consists of three parts, the control parameter of standard map *K*, the control parameter of Chebyshev map *k*, and the initial value of Chebyshev map x_0. According to the achievements in [25], most of the modern C/C + + compilers support a maximum of 64-bit integer types, the possible choices of *K* is around 9.2×10^{18}. For Chebyshev map, $x_0 \in [-1, 1]$ and *k* can have any real value greater than 2.0. According to the IEEE floating-point standard [32], the computational precision of the 64-bit double-precision number is about 10^{-15}, so the total number of possible x_0 is about 2×10^{15}. Though *k* can have any real value greater than 2.0 in theory, the range of *k* should be restricted to 2π to prevent Chebyshev map from producing periodic orbits, so the total number of the possible values of *k* is approximately $2\pi\times10^{15}$. Totally, the key space of the proposed cryptosystem is

$$Key_{total} = (9.2\times10^{18})\times(2\times10^{15})\times(2\pi\times10^{15}) \approx 2^{167},$$

which satisfies the key space requirements in [31], and is sufficiently large to resist brute attack.

4.2. Histogram Analysis

As mentioned before, histogram of a digital image shows the distribution information of the pixel values by plotting the number of pixels at each grayscale level. The ideal histogram of an effectively cipher image should be uniform and significantly different in comparison with that of the plain image. The histograms of the CT_Abdomen image and its cipher image are shown in figures 7(b) and 7(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 and consequently does not provide any clue to apply statistical attacks.

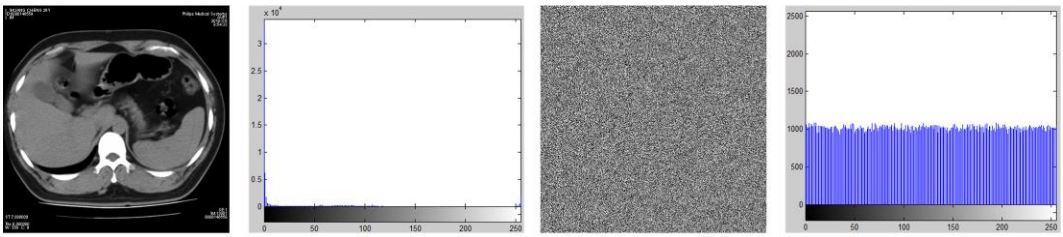


Figure 7. Histogram Analysis: (a) Plain Image; (b) Histogram of Plain Image; (c) Cipher Image; (d) Histogram of Cipher Image

4.3. Key Sensitivity Analysis

Except for large key space, extreme key sensitivity is another important issue to prevent brute-force attack. In this subsection, two kinds of tests are performed to evaluate the key sensitivity of the proposed scheme. (1) Encrypting the same plain image using slightly different secret keys; and (2) decrypting a cipher image using keys with tiny mismatch.

In consideration of the first case, we firstly encrypt the CT_Abdomen image with given coefficient *key*0=(*K*=512, *k*=9.87654321, x_0=0.123456789). Then a slight change is introduced to each of the parameter with all the others keep unchanged, and repeat 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 5. It is clear that a tiny difference in the key has caused substantial changes between the corresponding cipher images.

In addition, decryption using keys with slight difference are also performed so as to evaluate the key sensitivity of the second case. The deciphering images are shown in Figure 9. The differences between the incorrect deciphering images and the plain image are 98.90%, 99.59%, 99.61% and 99.60%, respectively.

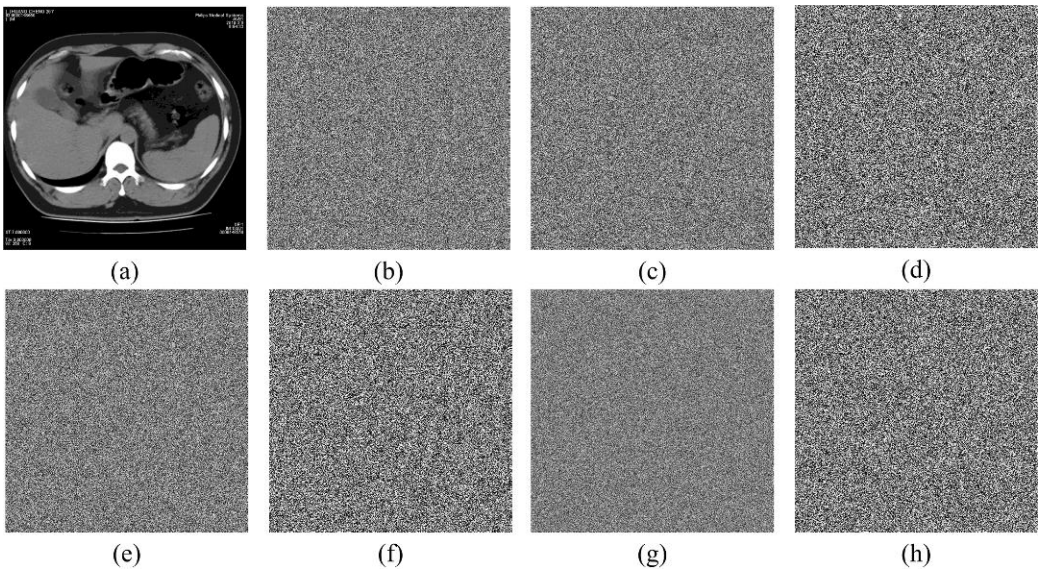
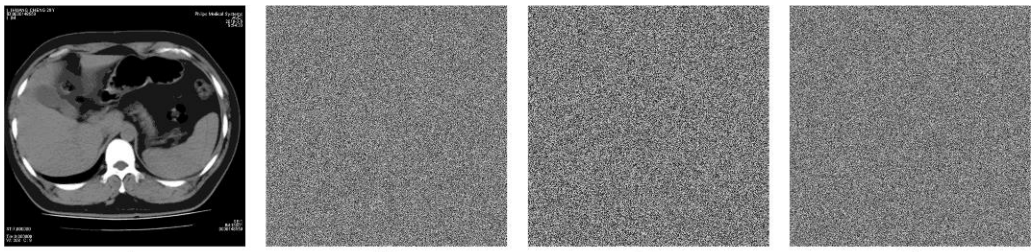


Figure 8. Key sensitivity test in the first case: (a) plain image; (b) cipher image (*K*=512, *k*=9.87654321, x_0=0.123456789); (c) cipher image (*K*=513,

k=9.87654321, x_0=0.123456789); (d) differential image between (b) and (c); (e) cipher image (K=512, k=9.87654321+10^{-14}, x_0=0.123456789); (f) differential image between (b) and (e); (g) cipher image (K=512, k=9.87654321, x_0= 0.123456789+10^{-14})

Table 5. Differences between Cipher Images Produced by Slightly Modified Keys

Figures	Encryption keys			Differences ratio between 8(b)
	K	k	x_0	
8(b)	512	9.87654321	0.123456789	—
8(c)	513	9.87654321	0.123456789	99.58%
8(e)	512	9.87654321+10^{-14}	0.123456789	99.62%
8(g)	512	9.87654321	0.123456789+10^{-14}	99.62%



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

Figure 9. Key sensitivity in the second case: (a) decipher image (K=512, k=9.87654321, x_0 = 0.123456789); (b) decipher image (K=513, k=9.87654321, x_0 =0.123456789); (c) cipher image (K=512, k=9.87654321+10^{-14}, x_0 =0.123456789); (e) decipher image (K=512, k=9.87654321, x_0 =0.123456789+10^{-14})

The above two tests indicate that the proposed image encryption scheme is highly sensitive to the secret key. Even an almost perfect guess of the secret key does not reveal any valuable information about the cryptosystem.

4.4. Correlation Analysis

The correlation between adjacent pixels in the plain image is always high for a meaningful image 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. To test this, 5000 pairs of adjacent pixels of the plain image and the cipher image are randomly selected from the horizontal, vertical and diagonal direction, respectively. The correlation coefficient r_{xy} of each pair are calculated according to the following three formulas:

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

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

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

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. To demonstrate this property graphically, the correlation of adjacent plain pixels in the three directions are depicted in figure 10. The dots are located along the diagonal in the plain image, whereas those of the cipher image are scattered over the entire plane. Besides, the correlation coefficients of the plain image and its cipher image are numerically listed in Table 6. It is obviously that the high correlation between adjacent pixels in the plain image has been significantly reduced in the cipher image.

Table 6. Correlation Coefficients of Adjacent Pixels

Direction	Plain image	Cipher image
Horizontal	0.9426	0.0090
Vertical	0.9506	0.0276
Diagonal	0.8951	0.0133

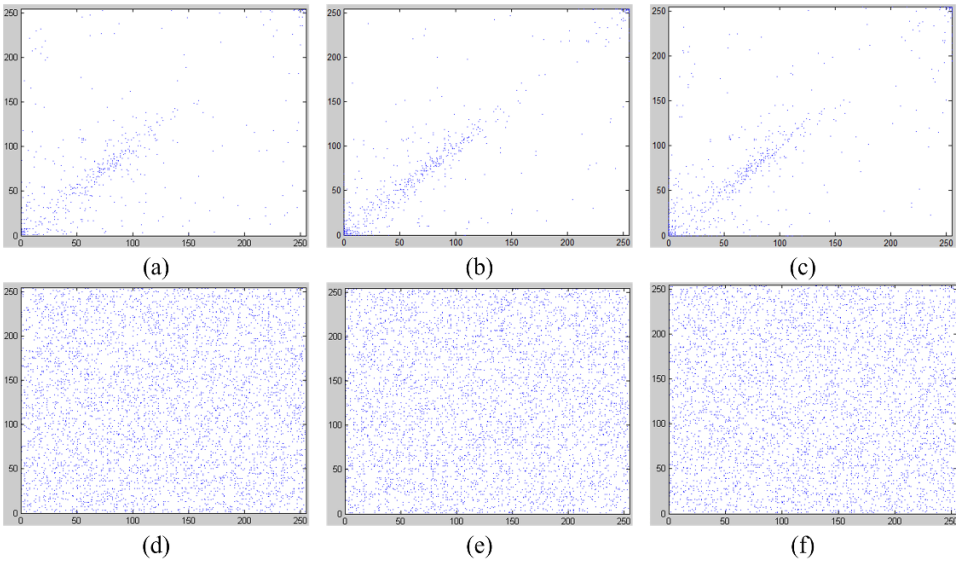


Figure 10. Correlation plot of two adjacent plain-image pixels in (a) horizontal, (b) vertical, (c) diagonal directions. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme in (d) horizontal, (e) vertical, (f) diagonal directions

4.5. Differential Attack

An effective image cryptosystem should spread out a slight modification in the plain image to a larger scale in the ciphered image, so as to resist differential attack. Two performance indices, *NPCR* (number of pixels change rate) and *UACI* (unified average changing intensity) are generally utilized to numerically evaluate the effectiveness of an image cryptosystem. Supposed that $P_1(i, j)$ and $P_2(i, j)$ be the $(i, j)th$ pixel of two images P_1 and P_2, respectively, *NPCR* is defined as

$$NPCR = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i, j)}{W \times H} \times 100\%, \quad (9)$$

where W and H are the width and length of P_1 and P_2 and $D(i, j)$ is

$$D(i, j) = \begin{cases} 0 & if \quad P_1(i, j) = P_2(i, j) \\ 1 & if \quad P_1(i, j) \neq P_2(i, j) \end{cases}. \tag{10}$$

UACI is defined as

$$UACI = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{|P_1(i, j) - P_2(i, j)|}{L-1}\right] \times 100\%. \tag{11}$$

The proposed cipher is implemented to all of the medical images and their modified version obtained by altering the last bit of the pixel in the lower right corner so as to evaluate the differential attack resistance. The results are listed in Table 7.

Table 7. Differential Attack Performance

Test image	1 Round		2 Rounds		3 Rounds		4 Rounds	
	NPCR(%)	*UACI*(%)	*NPCR*(%)	*UACI*(%)	*NPCR*(%)	*UACI*(%)	*NPCR*(%)	*UACI*(%)
CT_Abdomen	0.20	0.02	99.66	32.90	99.62	33.46	99.62	33.47
CT_Head	0.20	0.02	99.78	33.00	99.61	33.43	99.62	33.47
CT_Paranasal-sinus	0.20	0.05	99.40	33.79	99.58	33.46	99.63	33.41
MR_Cervical-vertebra	0.20	0.01	99.47	33.20	99.60	33.43	99.61	33.46
MR_Knee	0.20	0.05	99.60	33.44	99.61	33.41	99.59	33.44
MR_Prostate	0.20	0.01	99.47	33.20	99.60	33.43	99.61	33.46
MR_Waist	0.20	0.01	98.84	34.37	99.61	33.43	99.63	33.41
X_Lungs	0.20	0.01	99.59	33.44	99.61	33.50	99.62	33.46
Average	0.20	0.02	99.48	33.42	99.60	33.44	99.61	33.45

Based on the results, one can see that from the second round encryption, the one bit difference in the plaintext has spread out to a large part in the ciphertext. It is fully vindicated that our scheme has a steady and satisfactory security performance. In this scenario, differential will become infeasible, and the cryptosystem is thus more secure.

4.6. Information Entropy

Entropy is a significant property that reflects the randomness and the unpredictability of an information source, it was firstly proposed by Shannon in 1949 [29]. The entropy $H(s)$ of a message source s is defined in Eq. (12), 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 consists 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.

$$H(s) = -\sum_{i=0}^{2^N-1} P(s_i)\log_2 P(s_i). \tag{12}$$

All of the medical images are encrypted with the proposed cryptosystem. The information entropies of the cipher images are calculated, as listed in Table 8. 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 attacks.

Table 8. Entropies of Plain Images and Cipher Images

Test image	Plain images	Cipher images
CT_Abdomen	1.675035	7.999297339

CT_Head	2.683179	7.999272504
CT_Paranasal-sinus	3.328586	7.999249795
MR_Cervical-vertebra	6.323128	7.999242006
MR_Knee	5.384937	7.999265631
MR_Prostate	6.241683	7.999307430
MR_Waist	6.120326	7.999355484
X_Lungs	6.966350	7.999343550
Average	5.292598	7.999291717

5. Conclusions

In this paper, we present an efficient cryptosystem for medical image encryption. It is based on permutation-diffusion architecture, whereas an improved confusion approach is developed. The proposed permutation strategy can contribute certain pixel value modification effect and bit distribution balancing performance while maintaining a satisfactory image confusion effect. Collaborating with an image diffusion module, a complete cryptosystem is developed. Simulation and security analyses have proved the higher security level of the proposed cryptosystem, which renders it a good candidate for online medical applications.

Acknowledgements

This work was supported by Programs for Science and Technology Development of LiaoNing Province (No. 2013225036-13; No. 2013225089).

References

[1] J. K. Hu and F. L. Han, "A pixel-based scrambling scheme for digital medical images protection", J. Network Comput. Appl., vol. 32, no. 4, (**2009**).
[2] D. Bouslimi, G. Coatrieux and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: Application to echographic images", Compu. Meth. Prog. Bio., vol. 106, no. 1, (**2012**).
[3] M. Li, R. Poovendrana and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment", Comput. Med. Imag. Grap., vol. 29, no. 5, (**2005**).
[4] J. Montagnat, F. Bellet, H. Benoit-Cattin, V. Breton, L. Brunie, H. Duque, Y. Legr´e, I.E. Magnin, L. Maigne, S. Miguet, J. -M.Pierson, L. Seitz and T. Tweed, "Medical images simulation, storage, and processing on the European Data Grid testbed", J. Grid Comput., vol. 2, no. 4, (**2004**).
[5] United States Department of Health and Human Services. HIPPA: medical privacy—national standards to protect the privacy of personal health information. Available from: http://www.hhs.gov/ocr/hippa.
[6] F. Cao, H. K. Huang and X. Q. Zhou, "Medical image security in a HIPPA mandated PACS environment", Comput. Med. Imag. Grap., vol. 27, no. 2, (**2003**).
[7] HEMA, DICOM: digital imaging and communication in medicine. Available from: http://medical.nema.org/.
[8] Y. Zhang and D. Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption", AEU-Int. J. Electron. C., vol. 68, no. 14, (**2014**).
[9] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", Int. J. Bifurcat. Chaos, vol. 8, no. 6, (**1998**).
[10] 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 Dyn., vol. 77, no. 4, (**2014**).
[11] J. X. Chen, Z. L. Zhu, C. Fu and H. Yu, "An Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption", Math. Probl. Eng., vol. 2014, Article ID 427349 Doi: 10.1155/2014/427349, (**2014**).
[12] S. Behnia, A. Akhshani, H. Mahmodi H and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps", Chaos Solitons Fractals, vol. 35, no. 2, (**2008**).
[13] C. Li, Y. Liu, T. Xie, M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences", Nonlinear Dynamics, vol. 73, no. 3, **(2013)**.
[14] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos", Phys. Lett. A, vol. 372, no. 4, (**2008**).

[15] J. X. Chen, Z. L. Zhu and H. Yu, "A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme", Optik, vol. 125, no. 11, (**2014**).
[16] G. R. Chen, Y. B. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos Solitons Fractals, vol. 21, no. 3, (**2004**).
[17] Y. Wang, K. W. Wong, X. F. Liao, T. Xiang and G. R. Chen, "A chaos-based image encryption algorithm with variable control parameters", Chaos Solitons Fractals, vol. 41, no. 4, (**2009**).
[18] G. Ye and K.W. Wong, "An image encryption scheme based on time-delay and hyperchaotic system", Nonlinear Dyn., vol. 71, no. 1-2, (**2013**).
[19] J. X. Chen, Z. L. Zhu, C. Fu and H. Yu, "An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism", Opt. Express, vol. 21, no. 23, (**2013**).
[20] 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 Process-Image., vol. 28, no. 3, (**2013**).
[21] Y. B. Mao, G.R. Chen and S. G. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps", Int. J. Bifurcat. Chaos, vol. 1 4, no. 10, (**2004**).
[22] Y. S. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion", Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 1, (**2014**).
[23] Y. Zhang and D. Xiao, "Self-adaptive permutation and combined global diffusion for chaotic color image encryption", AEU-Int. J. Electron. C., vol. 68, no. 14, (**2014**).
[24] C. Fu, B. B. Lin, Y. S. Miao, X. Liu and J. J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption", Opt. Commun., vol. 284, no. 23, (**2011**).
[25] C. Fu, J. J. Chen, H. Zou, W. H. Meng, Y. F. Zhan and Y. W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy", Opt. Express, vol. 20, no. 3, (**2012**).
[26] C. F. Lin, C. H. Chung and J. H. Lin, "A chaos-based visual encryption mechanism for clinical EEG signals", Med. Biol. Eng. Comput., vol. 47, no.7, (**2009**).
[27] C. Fu, W. H. Meng, Y. F. Zhan, Z. L. Zhu, F. C. M. Lau, C. H. Tse and H. F. Ma, An efficient and secure medical image protection scheme based on chaotic maps, Compu. Bio. Med., vol. 43, no. 8, (**2013**).
[28] M. Zanin and A. N. Pisarchik, "Gray code permutation algorithm for high-dimensional data encryption", Inform. Sci., vol. 270, no. 20, (**2014**).
[29] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell .Syst. Tech. J., vol. 28, no. 4, (**1949**).
[30] W. Zhang, K.W. Wong, H. Yu and Z. L. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions", Commun. Nonlinear Sci. Numer. Simul., vol. 18, no. 3, (**2013**).
[31] G. Alvarez and S.J. Li, Some basic cryptographic requirements for chaos-based cryptosystem, Int. J. Bifurcat. Chaos, vol. 16, no. 8, (**2006**).
[32] IEEE Computer Society, IEEE standard for binary floating-point arithmetic. ANSI/IEEE std., August 754-1985, (**1985**).

Authors

Li-bo Zhang, He is an expert in medical image processing, online diagnosis, in department of radiology, General Hospital of Shenyang Military Area Command. He is now purchasing his doctor's degree in Software College, Northeastern University, Shenyang, China.

Ben-qiang Yang, He is now the dean of department of radiology, General Hospital of Shenyang Military Area Command. His research interest includes image processing, online diagnosis, and biomedical imaging.

