Signal Processing 132 (2017) 96–109

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Medical image encryption using edge maps

Weijia Cao[a], Yicong Zhou[a,*], C.L. Philip Chen[a], Liming Xia[b]

[a] Department of Computer and Information Science, University of Macau, Macau, China
[b] Department of Radiology, Tongji Hospital, Tongji Medical College, Huazhong University of Science and Technology, Wuhan 430030, China

ARTICLE INFO

Keywords:
Bit-plane decomposition
Chaotic map
Edge map
Medical image encryption

ABSTRACT

This paper presents a medical image encryption algorithm using edge maps derived from a source image. The algorithm is composed by three parts: bit-plane decomposition, generator of random sequence, and permutation. It offers users the following flexibilities: (1) any type of images can be used as the source image; (2) different edge maps can be generated by various edge detectors and thresholds; (3) selection of appropriate bit-plane decomposition method is flexible; (4) many permutation methods can be cascaded with the proposed algorithm. A significantly large key space and strong key sensitive are possessed by the proposed algorithm to protect different types of medical images. Furthermore, it has a wider applicability than other methods for fuzzy edge maps. Experiments and security analysis further demonstrate that it has a strong resistance against various security attacks and outperforms other state-of-the-art methods.

1. Introduction

Medical diagnostics are based on ultrasound, computed tomography, magnetic resonance imaging, positron emission tomography, and other techniques. The diagnostic images are extensively stored and transmitted for some specific purposes, such as feature selection [1], image denoising [2], segmentation [3], data hiding [4], and compression [5]. Moreover, the medical images are often distributed via an intranet of hospital or internet with a lot of confidential information related to patients' privacy. However, intranet of hospital are lacking serious security instruments and the internet also suffer serious issues like malicious tampering and privacy leakage [6–8].

Encryption of medical image is an effective way to prevent medical images from the threats [9]. Some conventional encryption methods, such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA), are originally employed for securing textual data. However, the methods have been found to be not suitable for digital images because of their intrinsic features like high pixel redundancy and correlation [10]. To reduce the redundancy and correlation, some researchers propose selective encryption algorithms. For example, some encrypt the important compressing coefficients [11–13]. Some others encrypt interleaved patient information of images [14], and use a stream cipher to encrypt only the significant bits of individual coefficients [15]. However, the methods cause some data loss and lead some negative misdiagnosis. Recently, to protect the integrity of medical image, Bouslimi proposes a joint watermarking/encryption system in Cipher-block chaining mode (CBC) [16], and designs a medical image encryption algorithm by merging a stream cipher algorithm and two substitutive watermarking approaches [17]. They can maintain the integrity and authenticity of an image. Some other algorithms propose pixel arrangement and use chaotic maps [18–20]. However, the techniques are not suitable for bulky data, e.g. medical images, and they are vulnerable to the differential attack because of their low security level.

To overcome the above problems, we propose a medical image encryption algorithm based on edge maps, named EMMIE. It employs three flexible parts, including bit-plane decomposition methods, generator of chaotic sequence, and scrambling method. In the lossless process, EMMIE possesses the computational efficiency since binary edge maps and bit-plane decomposition are efficiently operated by a digital computer [21]. A new permutation method involved in the process can change both position of bits and values of pixels, which can further improve the security level of EMMIE [22]. Simulation results and security analysis demonstrate the effectiveness and promising performance of EMMIE.

The rest of this paper is organized as follows. Section 2 describes the proposed EMMIE in detail. Simulation results and security analysis are presented in Sections 3 and 4, respectively. Section 5 concludes the paper.

2. Medical image encryption algorithm using edge maps

In the section, we first briefly review edge maps. Considering the

* Corresponding author.
E-mail address: yicongzhou@umac.mo (Y. Zhou).

http://dx.doi.org/10.1016/j.sigpro.2016.10.003
Received 2 March 2016; Received in revised form 22 September 2016; Accepted 3 October 2016
Available online 06 October 2016

edge maps as security keys, an edge map-based medical image encryption (EMMIE) algorithm is proposed.

2.1. Introduction of edge maps

Edge detection is a set of mathematical approaches to extract some points of high contrast by computing intensity differences in a digital image. Formally, the points constitute an edge map of an image. Therefore, an edge map presents the features and boundary of an object or a surface between two areas within an image [23]. It is widely used in many fields including image denoising [24], image enhancement [25], and feature extraction [26]. In EMMIE, edge maps are the first time to be proposed for medical image encryption.

Some edge detectors are usually applied to generate edge maps of $2D$ images, e.g. Prewitt, Sobel and Canny detectors [27]. They use two masks, M_r and M_c, which are convolved with an image I to detect derivative approximations of its rows and columns, G_r and G_c. Mathematically, the function can be defined as

$$G_r = M_r * I,\ G_c = M_c * I,$$

where * denotes one dimensional convolution operation. Then, the gradient magnitude G at each point and the direction θ of that gradient are given by

$$G = \sqrt{G_r^2 + G_c^2},\ \theta = \arctan\left(\frac{G_r}{G_c}\right).$$

Edge maps are plotted by the gradient magnitudes with different edge detectors. Prewitt detector often operates the gray weighted algorithm with the neighbor points and detects the edge when the value reach a peak point [27]. Its row mask is

$$M_{rp} = \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{pmatrix}$$

and the column mask is

$$M_{cp} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{pmatrix}.$$

Similarly, the Sobel detector uses other two masks: the row mask

$$M_{rs} = \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix}$$

and the column mask

$$M_{cs} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix}.$$

Canny detector is a derivative of the Gauss function and it can obtain good balance between noise suppression and edge detection. An image using Canny detector is firstly smoothed by Gauss filter, and finds the intensity gradients of the image using convolution masks of

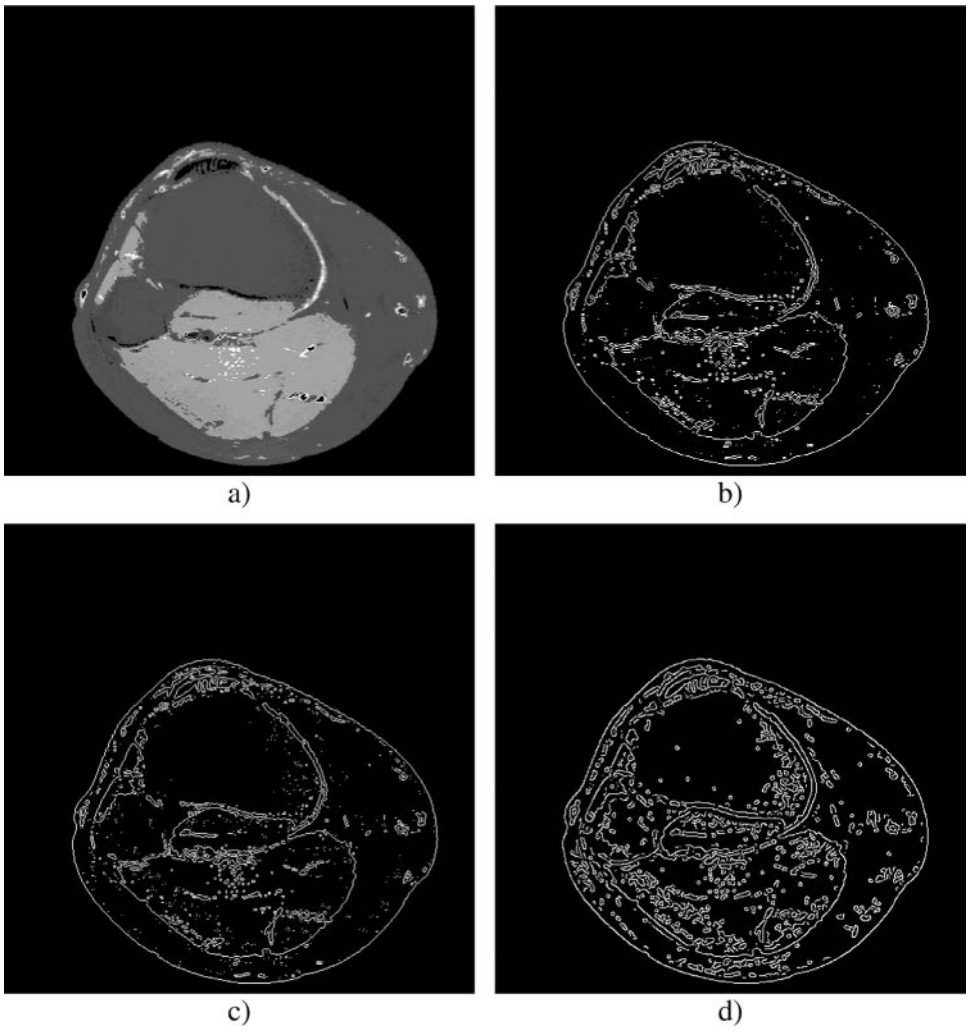

Fig. 1. Edge maps generated by different edge detectors with the same threshold 0.01: (a) a medical image; (b) edge map generated by Prewitt detector; (c) edge map generated by Sobel detector; (d) edge map generated by Canny detector.

other edge detectors, e.g. Sobel and Prewitt detectors. Then it calculates the gradient approximations and the directions by non-maxima suppression, and uses the double thresholding algorithm to detect and link edges, which are elaborated in [28]. Canny detector is one of the best edge detectors for its low error rate and strong denoising capability. Fig. 1(b)–(d) shows different edge maps using the above edge detectors. Different edge maps can be generated by various edge detectors and parameters. Moreover, they are binary images which can easily perform operations with bit planes of an image. Therefore, edge maps are chosen as the security keys in EMMIE owing to the advantages.

2.2. Description of EMMIE

The flowchart of EMMIE is shown in Fig. 2. A medical image to be encrypted is firstly decomposed into some bit-planes with a reversible decomposition method. The edge maps are generated from a source image with same or different thresholds and they are binary images with the same size as the original bit-planes. Then EMMIE performs an XOR operation between the bit-planes and edge maps. Finally, bit positions of all XORed-bit-planes are scrambled and then combined together with a pixel diffusion to compose cipher-image. The decryption is the inverse process of the above steps.

EMMIE is composed by three parts: bit-plane decomposition, generator of random sequence and edge map, and permutation. First, EMMIE decomposes the original medical image into n bit-planes by different methods, e.g. Binary bit-plane decomposition, Fibonacci P-code Bit-planes Decomposition [29] and Truncated Fibonacci P-code Bit-planes Decomposition [21]. For a gray-scale image, the 15 bit planes are generated by Fibonacci P-code bit-plane decomposition and the 14 bit-planes are generated by Truncated Fibonacci P-code bit-plane decomposition with p=2. A 16-bit-level medical image can be decomposed as 16 bit planes by Binary bit-plane decomposition.

Secondly, EMMIE generates n edge maps with thresholds produced by a chaotic map. These n edge maps can be the same or different with thresholds $p_1, p_2, \cdots, p_n$. Here we assume that there are m different edge maps derived from m various thresholds (i.e. m is an integer selected from 1 to n). To achieve a better random performance, any chaotic map can be cascaded in EMMIE. It chooses the Double-Sine map as the default chaotic map, which can be defined as

$$x_{k+1} = d\sin(\pi c \sin(\pi x_k)), \tag{1}$$

where k is a non-negative integer and $k \in [0, m]$, c, $d \in [0, 1]$ [30]. With parameter c=0.9, d=0.1 and initial value $x_0 = 0.9$, the part generates a random sequence $\{x_1, x_2, \ldots, x_m\}$ by a chaotic map. The m numbers in the sequence are assigned to the n thresholds $\{p_1, p_2, \ldots, p_n\}$. The rule of assignment is user-defined. For example, it can be written as

$$p_j = x_i,\ i = (j-1) \bmod m + 1, \tag{2}$$

where $i \in [1, m]$, and $j \in [1, n]$. For example, if $n = 8$, $m = 3$, which means a random sequence $\{x_1, x_2, x_3\}$ is generated by a chaotic map. Then the values of thresholds $\{p_1, p_2, \ldots, p_8\}$ will be $\{x_1, x_2, x_3, x_1, x_2, x_3, x_1, x_2\}$ according to the Eq. (2). Choosing the thresholds $p_1, p_2, \ldots, p_n$, n edge maps can be generated from a source image. For simplicity, this paper uses a single edge map for each bit-plane, i.e. m=1.

After the n bit-planes perform XOR operation with the n edge maps, a bit-level scrambling algorithm is used to permute the bit positions of the XORed bit-planes including bit diffusion and then a pixel diffusion is applied.

The new scrambling method is based on Sine Map

$$x_{i+1} = q\sin(\pi x_i), \tag{3}$$

where $q \in [0, 1]$ [31,32]. The scrambling method includes the following steps:

(1) Rearrange the n XORed bit-planes $E(r, c, b)$ with a size of $S = r \times c \times b$ into $1D$ binary stream st=$\{st_1, st_2, \ldots, st_S\}$, where $st_{(r-1)S+c+(b-1)S/n} = E(r, c, b)$.
(2) Perform the XOR operation between two neighbour bits within st to do the bit diffusion. Here we use $sx_1 = st_1$, $sx_i = st_{i-1} \oplus st_i$, where $i \in [2, S]$.
(3) Count z which is the total number of ones in the first edge map

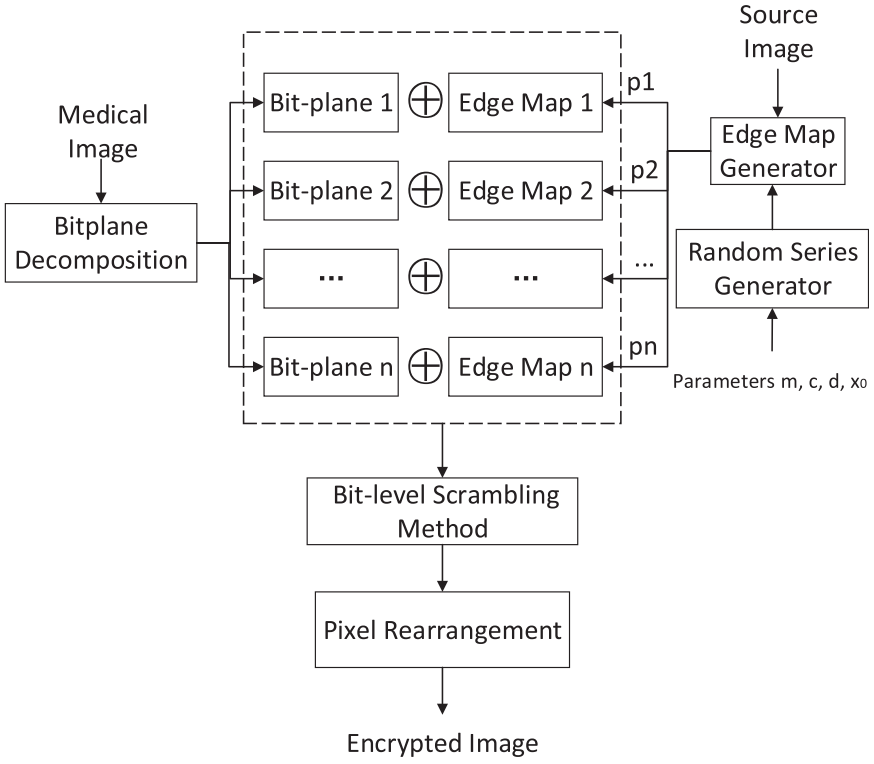

Fig. 2. The flowchart of EMMIE.

with the threshold p_1.

(4) Obtain the $z+1$ rounds of outputs of the Sine map with parameter q and initial value x_0 to form x_z.
(5) Iterate the Sine map with initial value x_z for S times to generate a chaotic sequence $\mathrm{A} = \{A_1, A_2, \ldots, A_S\}$.
(6) Sort the array A in ascending order and generate another array $\widehat{A} = \{\widehat{A}_1, \widehat{A}_2, \ldots, \widehat{A}_S\}$, which is a permutation of A.
(7) Sort the original binary stream sx to be a permuted stream $px = \{px_1, px_2, \ldots, px_S\}$, where $px_i = sx_j$ while $\widehat{A}_i = A_j$.
(8) Reshape the stream px into a $r \times c \times b$ encrypted bit-planes $\widehat{E}(r, c, b)$, where $\widehat{E}(r, c, b) = px_{(r-1)S+c+(b-1)S/n}$.

A pixel diffusion is selected in EMMIE after the scrambling bit-planes are combined as a noised image I_{ns} with a size of $N = r \times c$. Then reshape the I_{ns} into a $1D$ image ID where $ID_{(r-1)N+c} = I_{ns}(r, c)$ and assume the source image is $Isou$. Then the $1D$ diffused image Ic can be represented as

$$Ic_1 = (ID_1 + Isou_1) \bmod 2^n,\ Ic_i = (Ic_{i-1} + ID_i) \bmod 2^n, \tag{4}$$

where $i \in [2, N]$ and n is the number of bit-planes. Rearrange the Ic into a $r \times c$ image Ie that is the final cipher-image. Then the resulting cipher-image Ie is obtained after the bit-plane decomposition, the XOR operation with edge maps from source image, the scrambling algorithm, and final pixel diffusion.

In the decryption process, authorized users can reconstruct the original image with correct security keys: the source image $Isou$, the number of different edge maps m, edge detector and threshold, and the parameters of scrambling method.

First, it can be processed that the inverse of the final mod operation step. The $1D$ image Ier can be rearranged from the $r \times c$ image Ie and then $1D$ recovered image Ir takes the mod operation from image Ier which can be written as

$$Ir_i = (Ier_i - Ir_{i-1}) \bmod 2^n, \quad Ir_1 = (Ier_1 - Isou_1) \bmod 2^n, \tag{5}$$

where $i \in [2, N]$ and n is the number of bit-planes. Secondly, since the proposed scrambling method is a symmetric algorithm users can reverse the steps of it with correct parameters q, x_0 in order to get the n reconstructed XORed bit-planes. Then n bit-planes can be obtained after the n key edge maps with parameters m, c, d, x_0 to perform XOR operation with the XORed bit-planes. Finally, the recovered image can be generated after users combine the n bit-planes together.

2.3. Advantages of EMMIE

Unlike the key parameters or sequences used from other medical

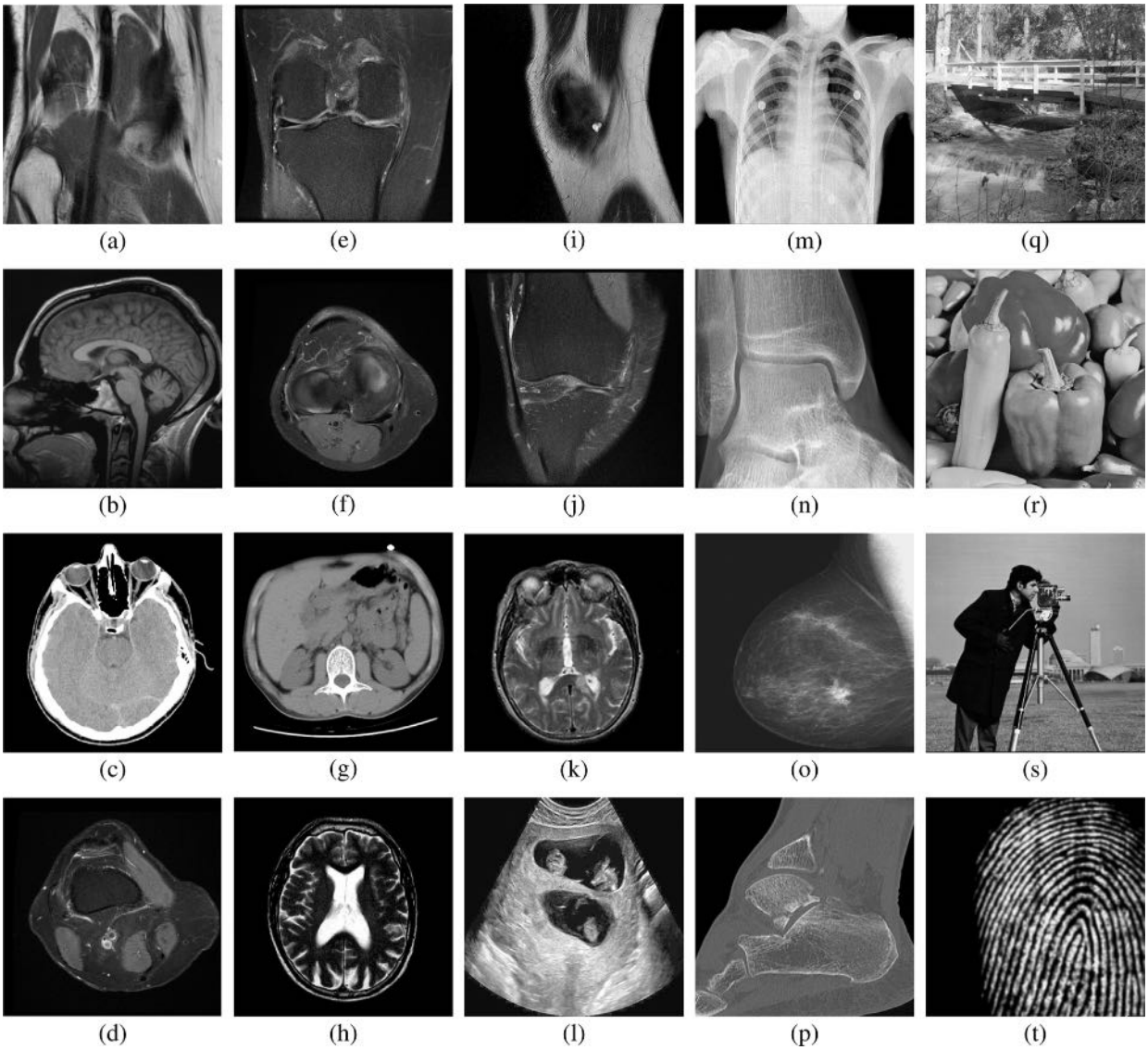

Fig. 3. Test images: (a)–(k) MRI images; (l) an US image; (m)–(n) X-ray images; (o)–(p) CT images; (q)–(s) grayscale images; (t) a biometric image.

image encryption algorithms, the keys mainly include the source image, the number of different edge maps, the edge detector and threshold, and the parameters of permutation method.

In the encryption process of EMMIE, arbitrary reversible bit-plane decomposition approach can be applied. The source image can be any image with the same size as the original image. The parameters of edge maps extracted from the source image can be generated by any chaotic map. These properties significantly increase the key space of EMMIE. In the decryption process, even that hackers possess the keys, they cannot recover the original image correctly, because they have to use the correct decomposition method to decompose the cipher-image.

In summary, EMMIE has five following flexibilities:

(1) It can flexibly select reversible decomposition methods for bit-plane decomposition.
(2) Any image can be considered as the source image.
(3) It can use any edge map detector and threshold to generate edge maps from the source image.
(4) Arbitrary chaotic map can be applied to generate the parameters of edge maps.
(5) It can shuffle the image bit or pixel positions by any scrambling algorithm.

3. Simulation results

In this section, we evaluate the encryption performance of EMMIE and then discuss the different results with various keys. Many medical images including MRI, X-ray, CT and US images are encrypted successfully by EMMIE. For simplicity, here we take twenty images shown in Fig. 3 as examples for our experiments and security analysis. In Fig. 3, the image sizes of Fig. 3(h), (k), (s), and (t) are 256× 256, and the sizes of other images are 512× 512.

In the experiment, if there is no special explanation, we use the binary bit-plane decomposition, the Double-sine chaotic map with the parameters g=1, c_0=0.9 and p=0.9. Then two aspects are shown our results as follows. One presents different types of medical images encrypted by EMMIE, and the other shows the experimental performance of EMMIE according to histograms of cipher-images.

3.1. Simulation results of EMMIE

An MRI image shown in Fig. 3(e) is encrypted by EMMIE with an edge map selected from another MRI image in Fig. 3(b). The encrypted MRI image shown in Fig. 4(b) is a noise-like image and totally different from the original MRI image. The distribution of the cipher-image's histogram is smooth, which means that EMMIE can defeat the statistical attacks. The recovered MRI image shown in the Fig. 4(c) is reconstructed without data loss since the original image and reconstructed image are exactly the same.

Moreover, the source image of EMMIE can be not only a medical image but also a natural image. For example, as shown in Fig. 5, the CT image taken from Fig. 3(p) is encrypted by an edge map extracted from a non-medical source image shown in Fig. 3(q). The cipher-image is unrecognized and its histogram distributes uniformly. The reconstruction is also lossless as is shown in Fig. 5(c) and (f).

EMMIE can also be applied to other medical images like X-ray and US images, which are taken from Fig. 3(n) and (l). The experimental results displayed in Fig. 6 show the original CT and US images can be completely recovered from a noised-like cipher-images.

3.2. Experimental performance of EMMIE

A uniform distribution of an cipher-image histogram can demonstrate a good encryption result so it can effectively prevent the attacks based on statistical analysis. To evaluate the performance of EMMIE, we compare the histogram distributions of different cipher-images using various keys described in Section 2. A large number of key edge maps can be generated from an image with different detectors or parameters as presented in Section 2.1 and most of them can be applied generally in different areas. However, some blurred edge maps are avoided in a lot of fields like image recognition or denoising. If encryption algorithm can take advantage of both blurred and unblurred edge maps, the flexibility of chosen keys for users can be largely improved and the security level also can be enhanced. Since EMMIE is

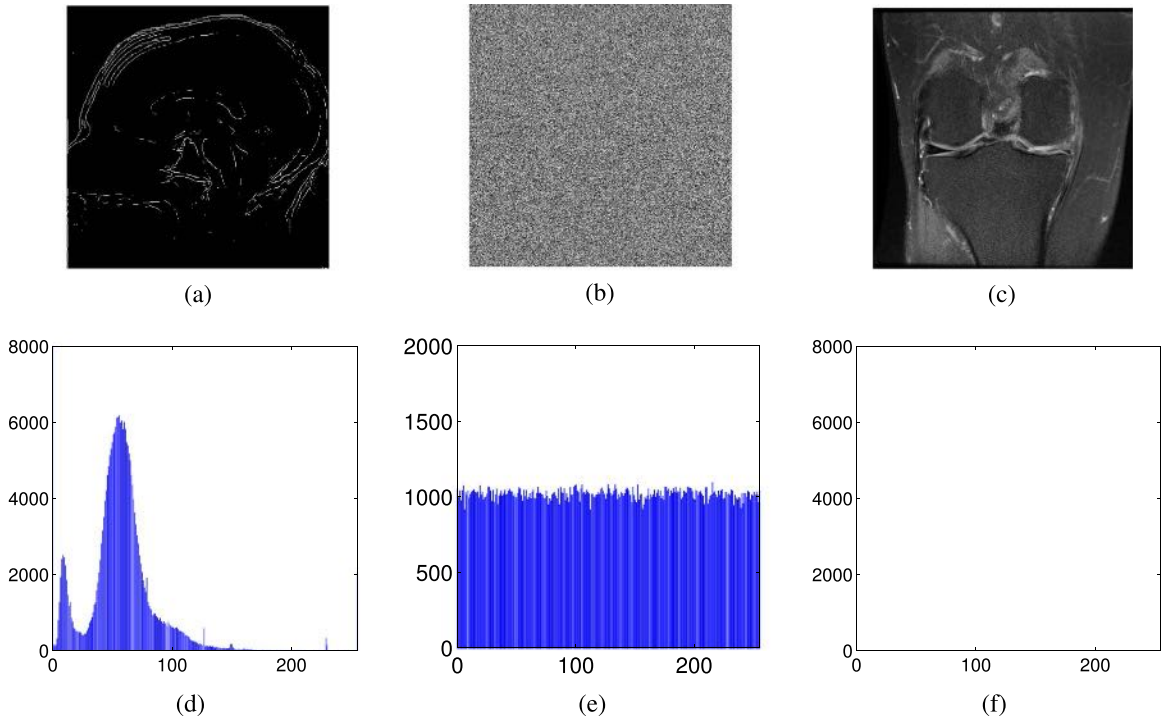

Fig. 4. EMMIE encryption results of the MRI image: (a) The edge map extracted from Fig. 3 (b) (Sobel detector); (b) the cipher-image; (c) the reconstructed MRI image; (d) the histogram of the original image shown in the Fig. 3 (e); (e) the histogram of (b); (f) the histogram of difference between the original image and (c).

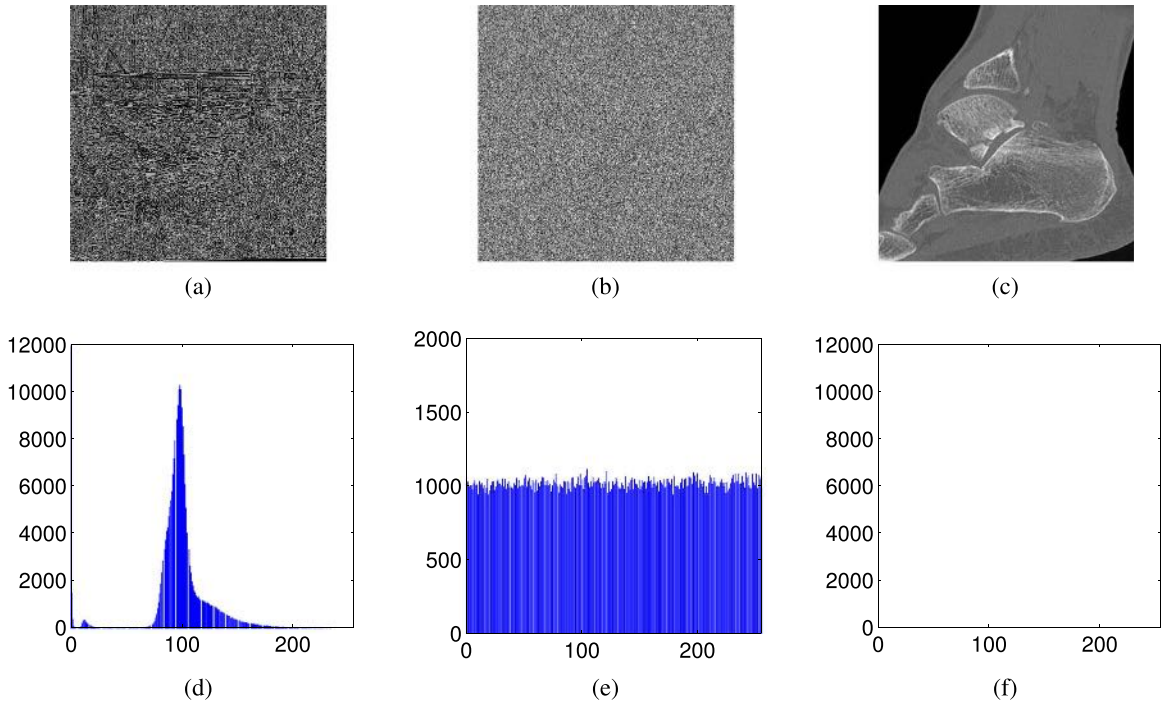

Fig. 5. EMMIE encryption results of the CT image: (a) The edge map extracted from Fig. 3 (q) (Sobel detector); (b) the cipher-image; (c) the reconstructed CT image; (d) the histogram of the original image shown in the Fig. 3(p); (e) the histogram of (b); (f) the histogram of the difference between the original image and (c).

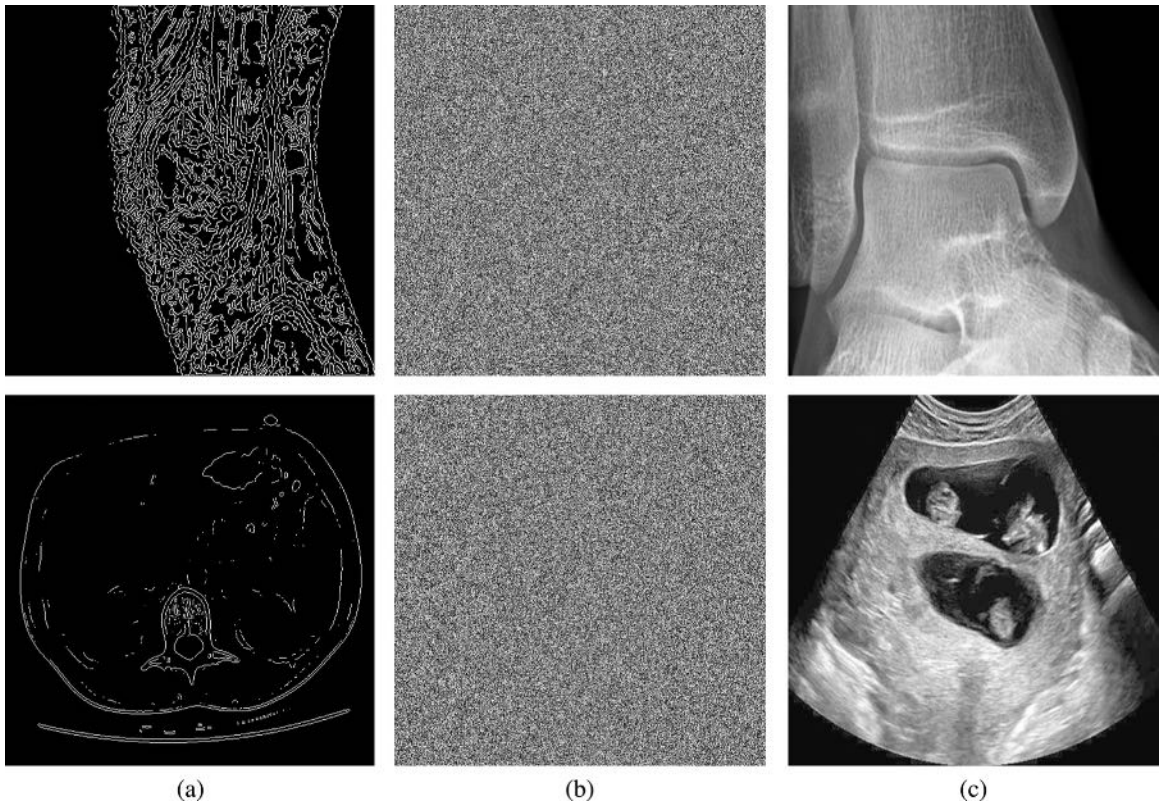

Fig. 6. EMMIE encryption results of the X-ray and US images. (a) The edge maps extracted from Fig. 3 (i) and (g) using Canny and Prewitt detectors; (b) the cipher-images of the original images shown in the Fig. 3 (n) and (l); (c) the recovered images.

based on a bit-level structure with lots of flexibilities as described in Section 2.3, it can diffuse the bit-level disturbances within or between the bit-planes of plain-image, which means it can obtain a significantly random cipher-image with different edge maps. Therefore, EMMIE can possess the flexibility to choose blurry or clear edge maps. Moreover, we carry out a thousand groups of experiments to verify our experimental performance and here we take some of them for examples.

As can be seen from Fig. 7, the histograms distribute differently with different edge maps. First, we choose the edge maps extracted from the source image shown in Fig. 3(m) with different edge detectors and the same threshold. We encrypt the original image with different edge maps generated by the previous step. The histograms of the

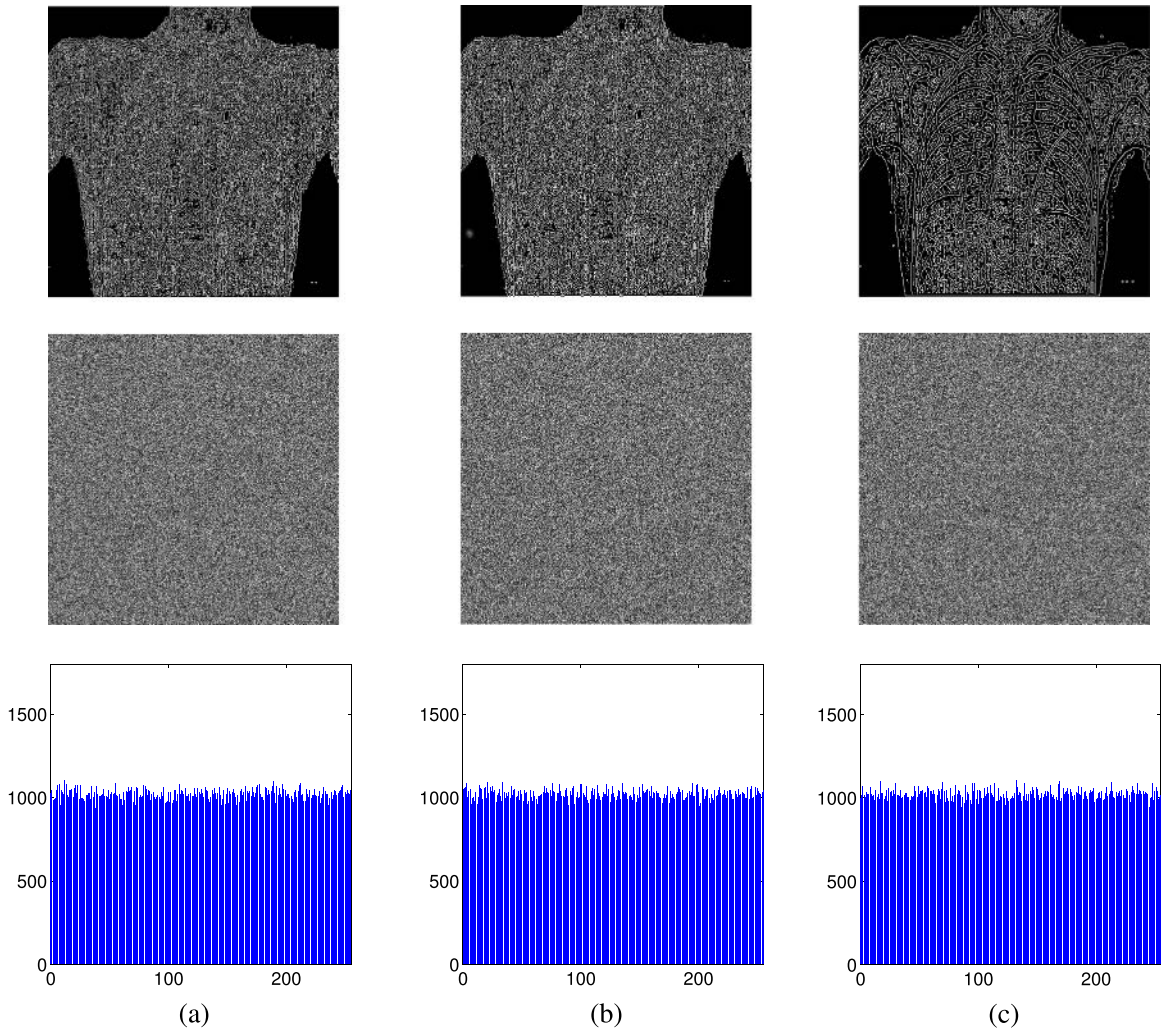

Fig. 7. The histograms of encrypted image using the edge maps with different detectors. An image (Fig. 3(a)) encrypted by edge maps extracted from Fig. 3(m) in the first row using different detectors with a threshold 0.02: (a) Prewitt, (b) Sobel, (c) Canny detectors, whose cipher-images and their histograms are shown in the last two rows.

cipher-images using all the three edge maps shown in Fig. 7(a)–(c) detectors have uniform distributions.

Secondly, the second row of Fig. 8 presents encryption results of the same original image using edge maps generated from the same source image with three thresholds, 0.1, 0.01, 0.001 and a same edge detector (i.e., Sobel detector). Their histogram results are shown in the last row. The histograms with all the thresholds show approximately a uniform distribution whether their edge maps are blurred or clear. Based on the above results, EMMIE can well utilize any edge map detector and threshold to generate edge maps. It increases the difficulty of hackers to break the keys combination. After a thousand groups of similar experimental results, we can conclude that EMMIE has a wider applicability whenever it uses a clear or blurred edge map.

Through the comparison results it is obvious that a blurry edge map may not be good for some image processing applications like image segmentation, but it can bring a good encryption performance, which means that EMMIE has a strong robustness for a fuzzy edge map. The universal applicability can enlarge the key space and improve the security level of EMMIE.

4. Security analysis

The security analysis is of great significance for an image encryption algorithm. To study the security level of EMMIE, this section analyses its performance from four aspects: key space, key sensitivity, analysis of pixel correlation, and differential attack.

4.1. Security key space

The totally possible combinations of the security keys of an image encryption algorithm form the security key space of the algorithm. The attackers can easily break the algorithm using the brute-force attack, when the key space of an algorithm is not sufficiently large. Therefore, a good image encryption algorithm requires a considerably large key space.

As mentioned in Section 2, the security key of EMMIE consists of four parts: the source image, the number of different edge maps, edge detector and threshold, and the parameter of scrambling method. The number of source images is significantly large because any grayscale image can be used as the source image. The edge detector can be used to generate edge maps in EMMIE. The threshold choices of the edge detector further increase the possible combinations of the security keys of EMMIE. Moreover, any scrambling algorithm can be applied to shuffle the bit positions. Therefore, the possible key combinations of EMMIE become increasingly various and then the key space of EMMIE is significantly large.

We can take an example to calculate the key space of EMMIE. We select an original medical image with size of $M \times N$ and pixel values within $[0, 2^q]$. Suppose the source image is taken from n_g gray images with the same size of the original image. Assume the edge detector is selected from m_t existing methods, e.g., Prewitt, Sobel, Canny detectors. Suppose there are m different edge threshold values for the m_t edge detectors, respectively. The totally possible choices of the edge

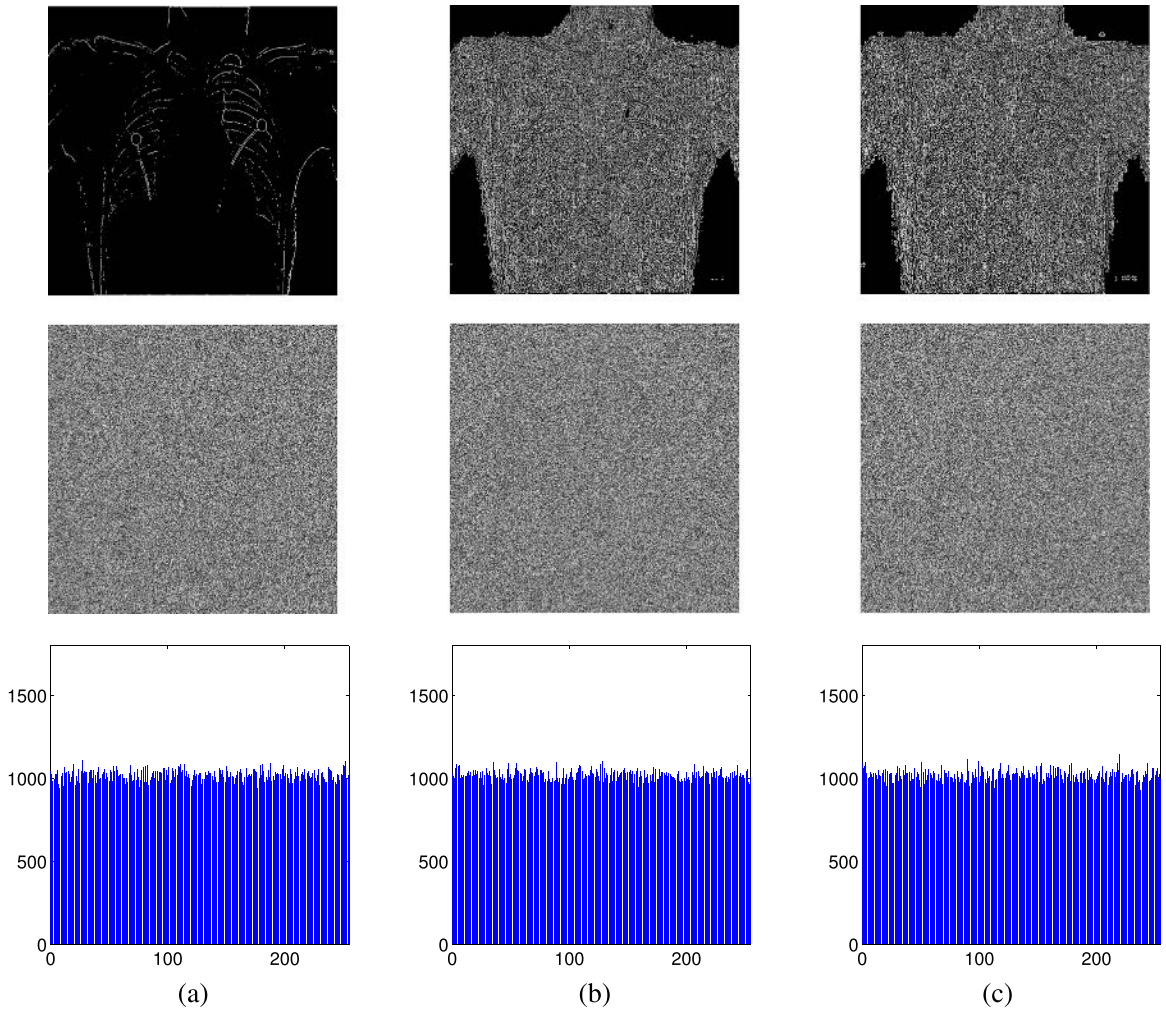

Fig. 8. The histograms of encrypted images using the edge maps with different thresholds. An image (Fig. 3(a)) encrypted by edge maps extracted from Fig. 3(m) using Sobel detector with different thresholds in the first row: (a) 0.1, (b) 0.01, (c) 0.001, whose cipher-images and their histograms are shown in the last two rows.

map will be $K_1 = n_g \times m_t \times m^q$. The scrambling algorithm can be any scrambling method and the possible changes of bit positions are $K_2 = M! \times N! \times q!$.

Therefore the key space of EMMIE is

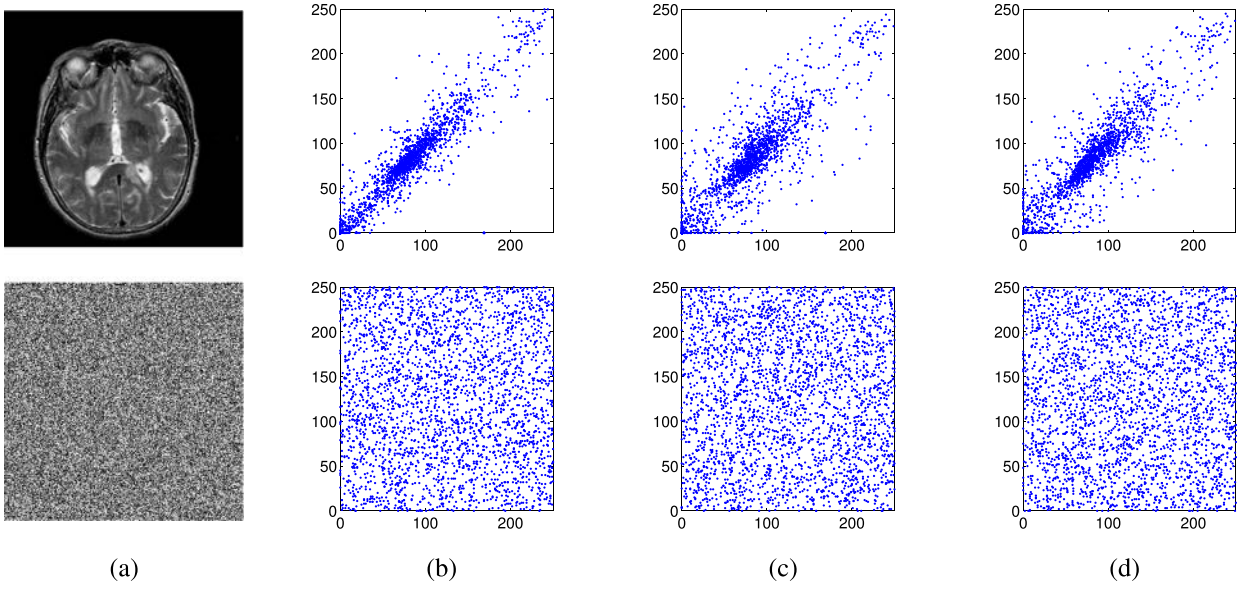

Fig. 9. Correlation analysis at different directions. The top and bottom rows plot the neighboring pairs of (a) the original image and cipher-image at the (b) horizontal, (c) vertical, and (d) diagonal directions, respectively.

$K = K_1 \times K_2 = n_g \times m_t \times m^q \times M!N!q!$. For example, assume a 8-bit-level medical image with the size of 100× 100 is to be encrypted, the source image is chosen from 5 grayscale images. Choose one of three detectors (i.e. Prewitt, Sobel, Canny detectors) with one of 5 different threshold values to generate edge map. The key space of EMMIE is $S = 5 \times 3 \times 5^8 \times 100! \times 100! \times 8! = 2.06 \times 10^{327}$. It proves that the key space of EMMIE is sufficiently large to withstand the brute-force attack.

4.2. Correlation analysis

Correlation analysis is a method to measure the randomness of an image. To prevent the leakage of the original information, an ideal random-like image often has a low correlation among its adjacent pixels. Mathematically, the coefficient correlation of two data sequences can be calculated by

$$corr(p, q) = \frac{E[(p - \mu_p)(q - \mu_q)]}{\sigma_p \sigma_q}, \quad (6)$$

where p is a pixel sequence and q is the corresponding neighboring pixels along with one of the horizontal, vertical and diagonal directions; μ_P and μ_q are the mean values of p and q; σ_P and σ_q denote the standard deviations of p and q; $E[\cdot]$ is the expected value. The absolute values of coefficients fall into the range of [0, 1]. The two sequences have a low correlation when their correlation absolute value is close to zero. Otherwise, it is close to one.

Here we use the original and source images as shown in Fig. 3(k) and (s) to do the image encryption for EMMIE. Then we measure the correlation of the adjacent pixels from the original and cipher-images, respectively. Randomly choosing 3000 pairs of neighbor pixels from original and cipher-images, we analyse correlation from the horizontal, vertical, and diagonal directions, respectively.

Since the process of EMMIE includes XOR operation and bit-level scrambling method, both the bit values and positions of its cipher-image are almost changed totally. The positions of the pixels of cipher-image will become unpredictable and random. Then the correlation between the neighbouring pixels of its cipher-image will be widely diminishing. As shown in Fig. 9, the horizontal axis means the concentration of the randomly selected pixels while the vertical axis shows the intensity of its corresponding neighboring pixels. The neighboring pixel pairs of the original image are distributed on or close to the diagonal line. It means that the neighboring pixels are equal or close to each other, which indicates a strong adjacent pixel correlation. On the other hand, the neighboring pixel pairs of the cipher-image distribute randomly in the whole data range. It means that the correlation of the cipher-image is extremely low.

To further evaluate the performance of EMMIE, we compare EMMIE with three image encryption methods: Zhou's scheme [33], Zhu's scheme [34], and DecomCrypt [21]. In our experiments, Zhou's scheme uses parameter (0.36, 3.65, 3, 2, 3, 2); Zhu's scheme takes (3.99999, 0.32, 0.8); and DecomCrypt uses the same source image as EMMIE with the 4th bit-plane. The adjacent pixel coefficient of the original image are listed in Table 1. After the image encryption, EMMIE makes a significant decorrelation of the neighboring pixels in the original image. Furthermore, EMMIE surpasses other three algorithms since its correlation coefficients are closer to zero.

4.3. Key sensitivity test

The sensitivity of the security key can measure how the encryption/decryption results of an encryption algorithm changes with different security keys. The hackers can easily use a similar key to break the image encryption algorithm with a low level of key sensitivity. Therefore, a high key sensitivity can provide a prior security level to the encryption algorithm.

The keys play a major role in the XOR operation, bit-level scrambling, and pixel shuffling parts of EMMIE. The space of keys is large and encrypted results are unpredictable. To evaluate the key sensitivity of EMMIE, we select the key edge maps from different source images or edge thresholds as examples. As shown in Fig. 10, we select the source image shown in Fig. 3(t) and its one-pixel-different image to generate two edge maps as shown in the top row of Fig. 10(a) and (b) using the Sobel detector with a threshold value 0.01. Then EMMIE uses the two edge maps to encrypt the original medical image as shown in Fig. 3 (h). Two cipher-images are presented in the bottom row of Fig. 10(a) and (b). Obviously, their difference in the bottom row of Fig. 10(c) is significantly larger than that of two source images or two edge maps. The rate of their different pixels is 99.65% (i.e. the number of pixel change rate). It demonstrates that a little change in the source image or edge map of EMMIE leads to a large difference in the cipher-image.

The key sensitivity of image decryption is presented in Fig. 11. Its source image is selected from Fig. 3(c). Here we generate the edge maps a and b shown in Fig. 11(a) and (b) using two different parameters of the edge detector Canny and their difference is only 0.01. First, we encrypt the original MRI image with the edge map c and the cipher-image is shown in Fig. 11(c). We then take the edge map b to recover the original image. Fig. 11(d) represents the decrypted image and Fig. 11(e) shows the correctly recovered image using the correct edge map a. It proves that we can correctly recover the original image only when we use the correct edge map. Therefore, the key sensitivity of EMMIE is also strong during its decryption process.

The mean square error (MSE) is always used to assess the difference between two images. To further evaluate quantitatively our performance in key sensitivity, we calculate the MSE values of the difference results in the encryption and decryption process, i.e. the difference between two cipther-images in the first row of Fig. 10(c) and between the recovered images in Fig. 11(d) and (e). Moreover, EMMIE is compared with other two algorithms of Zhu and DecomCrypt.

Table 2 shows the difference between the edges in Fig. 10(c) is tiny as the MSE value is few. The MSE values of EMMIE are the most of three schemes in both encryption and decryption of key sensitivity, which means the differences of them are more than other methods and it further proves that the key sensitivity of EMMIE is strong.

4.4. Histogram analysis

A histogram of an image is the intensity distribution of its pixels. A flat histogram of a cipher-image means it has a good randomness and it is able to resist statistic attacks. EMMIE is a bit-level encryption method, which can change randomly the bit values and positions of its cipher-image and then distribute uniformly the pixels of the cipher-image.

To further evaluate the performance of EMMIE in histogram distribution, we select the scheme of Zhou, Zhu, and DecomCrypt with the parameters described in Section 4.2 to do the comparison with EMMIE. The original image and source image are taken from Fig. 3(f) and (j).

Fig. 12 shows the simulation results of histogram analysis for the four image encryption schemes. The histogram of cipher-image by

Table 1
Correlation coefficients of the original image shown in the Fig. 9(a) and cipher-images using different encryption algorithms.

Orignal image and cipher-images	Horizontal	Vertical	Diagonal
Fig. 9(a)	0.9496	0.9554	0.9126
Zhu's [34]	−0.0124	−0.0038	−0.0090
Zhou's [33]	0.2725	−0.0256	−0.0661
DecomCrypt [21]	0.0285	−0.0350	−0.0102
EM−MIE	−0.0074	0.0019	−0.0017

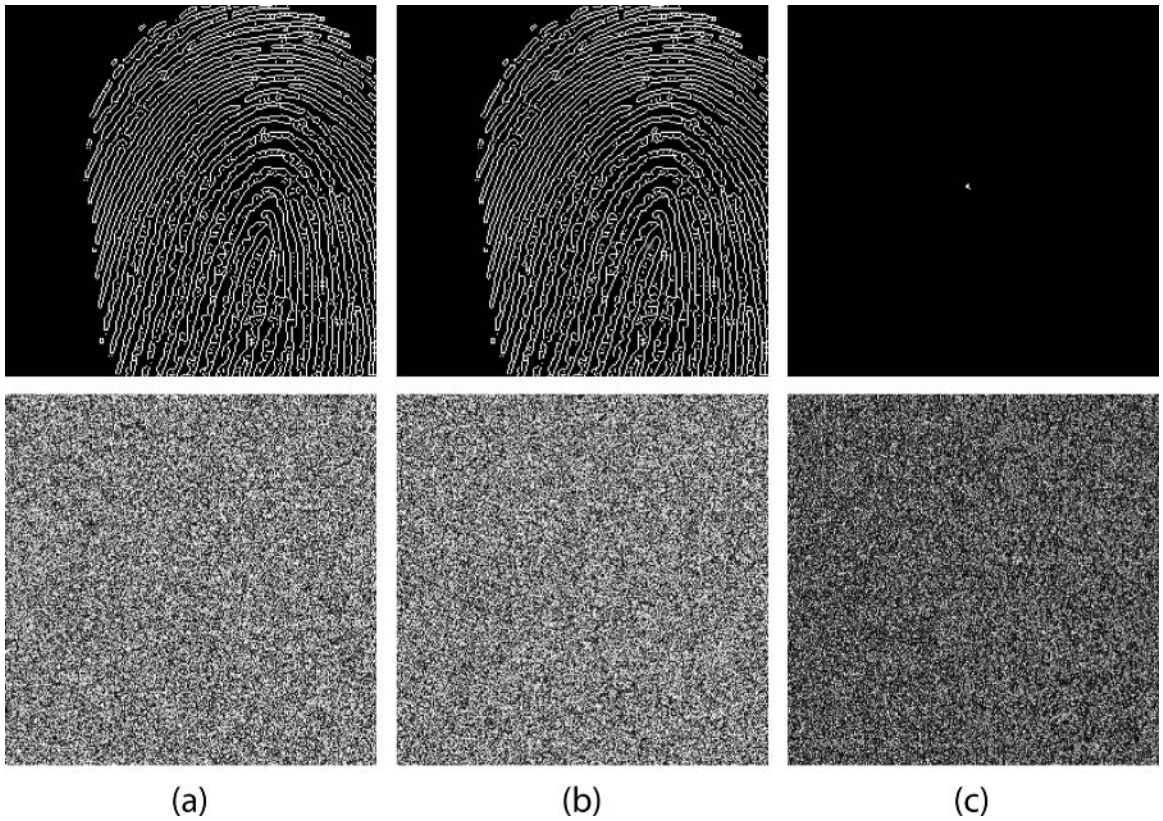

Fig. 10. Key sensitivity test for EMMIE encryption. (a) and (b) are two edge maps (Sobel detector, 0.01) extracted from a source image (Fig. 3(t)) and its one-pixel-different image, respectively, and their cipher-images shown in the last row. (c) is the difference between (a) and (b).

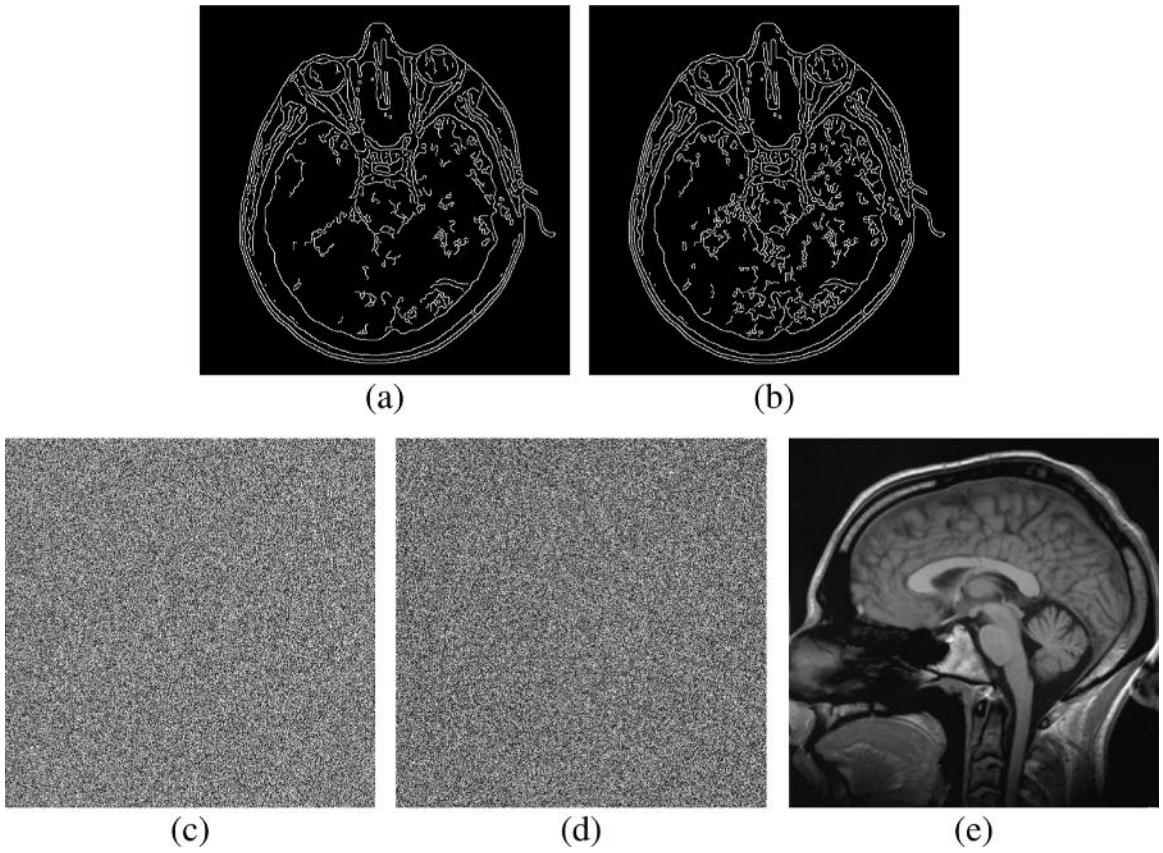

Fig. 11. Key sensitivity test for EMMIE decryption. (a) the edge map *a* (Canny detector, 0.1) and (b) the edge map *b* (Canny detector, 0.09) extracted from a same source image (Fig. 3 (c)); (c) the cipher-image using (a); (d) incorrectly recovered image using (b); (e) correctly recovered image using (a).

Table 2
Mean square errors of the key sensitivity test for the encryption and decryption processes of different encryption algorithms.

	Encryption	Decryption
The first row of Fig. 10(c)	0.00009	0.0097
Zhu's [34]	10914	3638
DecomCrypt [21]	7683.3	3480.5
EM-MIE	10968	11312

Zhou's method in Fig. 12(b) has nonuniform distribution as well as the DecomCrypt in Fig. 12(d). On the other hand, in Fig. 12(e), the histogram of EMMIE distributes almost equally as same as the Zhu's scheme in Fig. 12(c), which demonstrates that the histogram distribution of EMMIE has an equal or even better performance than other encryption schemes.

4.5. Time complexity analysis

This section analysis the encryption speed of EMMIE with different image sizes on an Intel Core i7 1.9 GHz with 16 GB RAM running on Windows 7 OS. EMMIE is a machine-friendly binary system based on edge maps, which can highly enhance the security efficiency. To evaluate the efficiency of EMMIE, three image encryption algorithms of Zhu, Zhou, and DecomCrypt are presented as comparisons in Fig. 13.

In Fig. 13, the original image and source image are selected from Fig. 3 (l) and (g), and the image size changes from 8 × 8 to 512× 512. As represented the encryption time of EMMIE, the blue curve in Fig. 13 is drawn from 0.0129 to 1.846 s with different image sizes, which is lower than other three schemes of Zhu, Zhou, and DecomCrypt. Therefore, the speed of EMMIE is faster than other state-of-the-art methods.

4.6. Error robustness analysis

The cipher-images may lost some data or be contaminated with noises when they are transmitted or stored. The decryption is correctly processed unless the encryption scheme has a strong robustness for these errors. On the other hand, users cannot obtain the final reconstructed image. Hence a good encryption algorithm should tolerate a certain level of errors.

EMMIE is an asymmetric encryption algorithm. In encryption process, one byte of the original image changed will spread over all

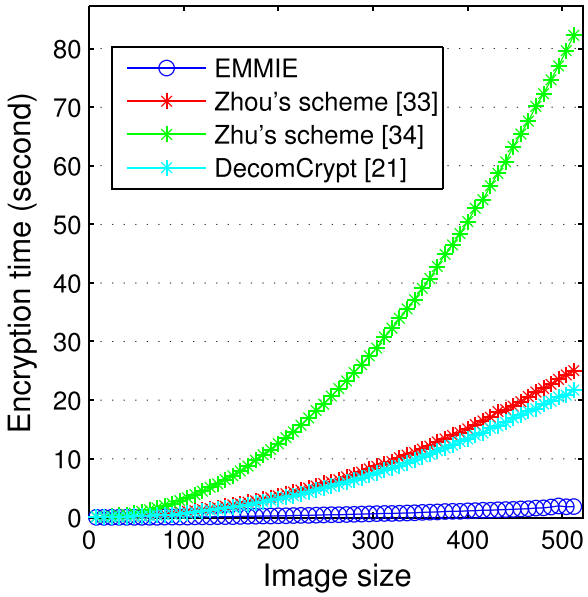

Fig. 13. The encryption time of the schemes of Zhu, Zhou, DecomCrypt and EMMIE with the increasing size of the original image in Fig. 3(l). The green, red, blue-green and blue lines represent the methods of Zhu, Zhou, DecomCrypt and EMMIE, respectively.

the bytes in the cipher-image. On the other hand, a change of a byte in the cipher-image can effect few bytes in the reconstructed image.

Figs. 14 and 15 show the data loss and noise robustness of the Zhou's algorithms, DecomCrypt, and EMMIE, respectively. The original images of them are selected from Fig. 3(e) and (o), and the source image are taken from Fig. 3(r) and (q). In Fig. 14(c), the decrypted image of EMMIE shows clearer than other two methods, as well as its recovered result of noise robustness in Fig. 15(c). Therefore, EMMIE has a certain tolerance for errors and performs a stronger robustness than other two algorithms.

4.7. Differential attack

The differential attack is also called the chosen-plaintext attack [35]. When an encryption algorithm can immune to the chosen-plaintext attacks, it is able to resist known-plaintext attacks and ciphertext-only as well [36]. The differential attack is an effective approach in which the hackers intend to break the encryption system using the differences of the cipher-images generated from the slightly-

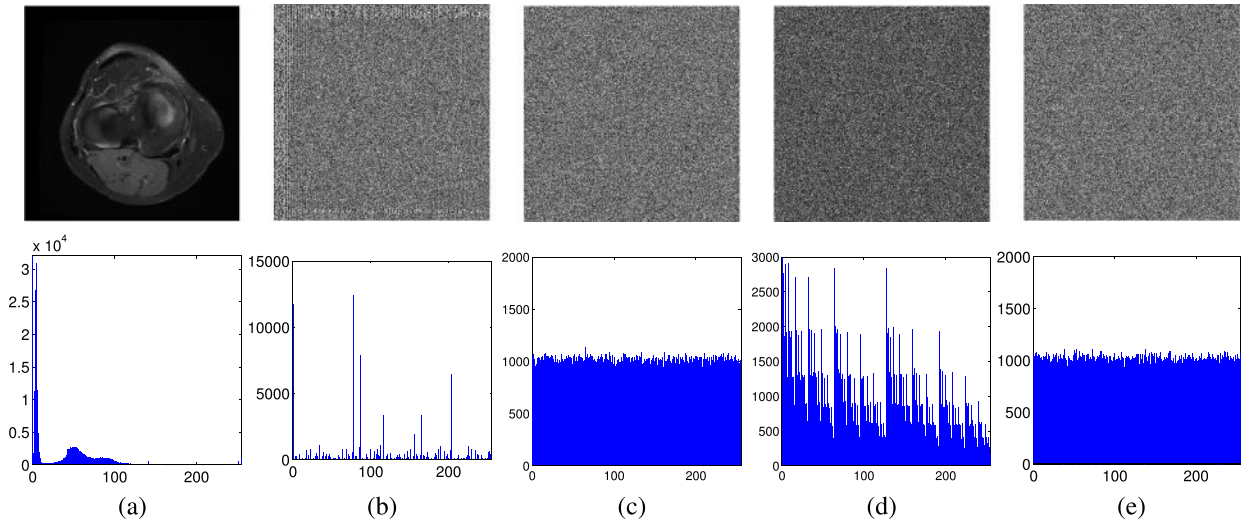

Fig. 12. Histogram analysis. (a) The original image and its histogram; (b)–(e) are the cipher-images and their histograms based on the schemes of (b) Zhou [33], (c) Zhu [34], (d) DecomCrypt [21], and (e) EMMIE.

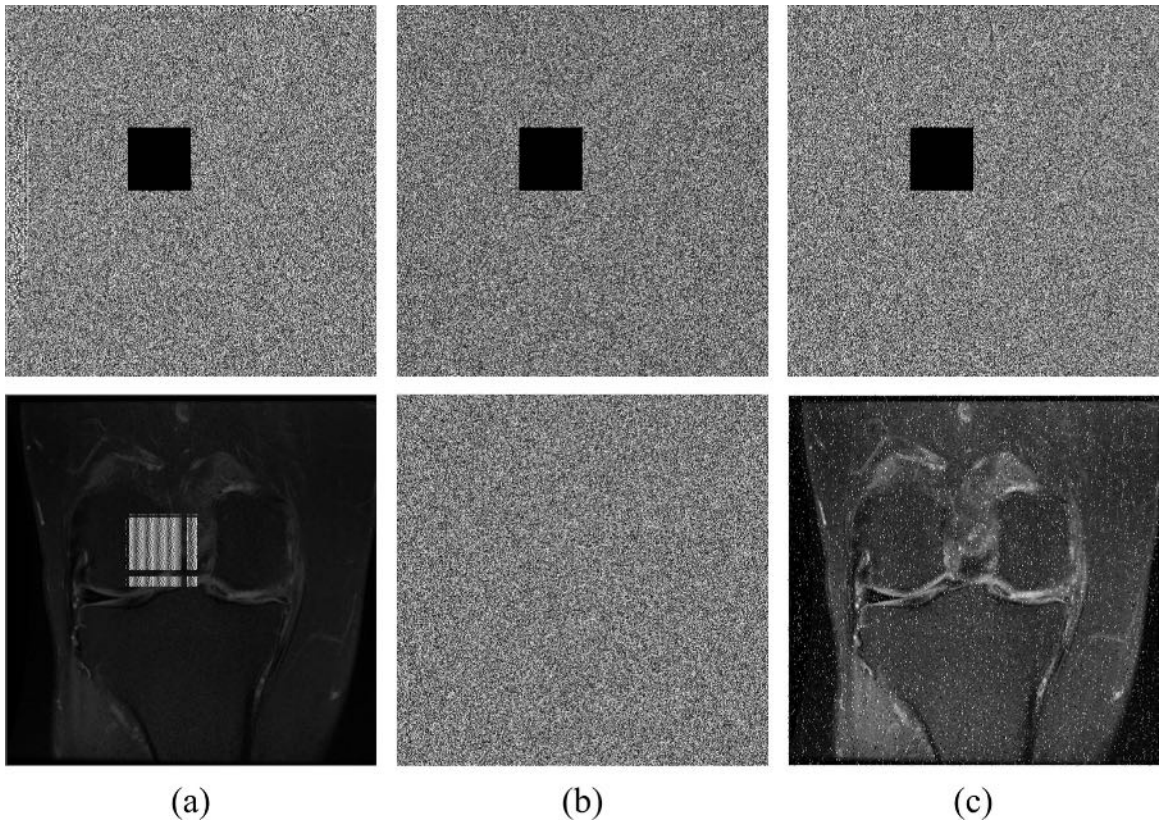

Fig. 14. Data loss robustness. (a)–(c) are the cipher-images with 3.3% data loss and their recovered images based on the schemes of (a) Zhou [33], (b) DecomCrypt [21], and (c) EMMIE.

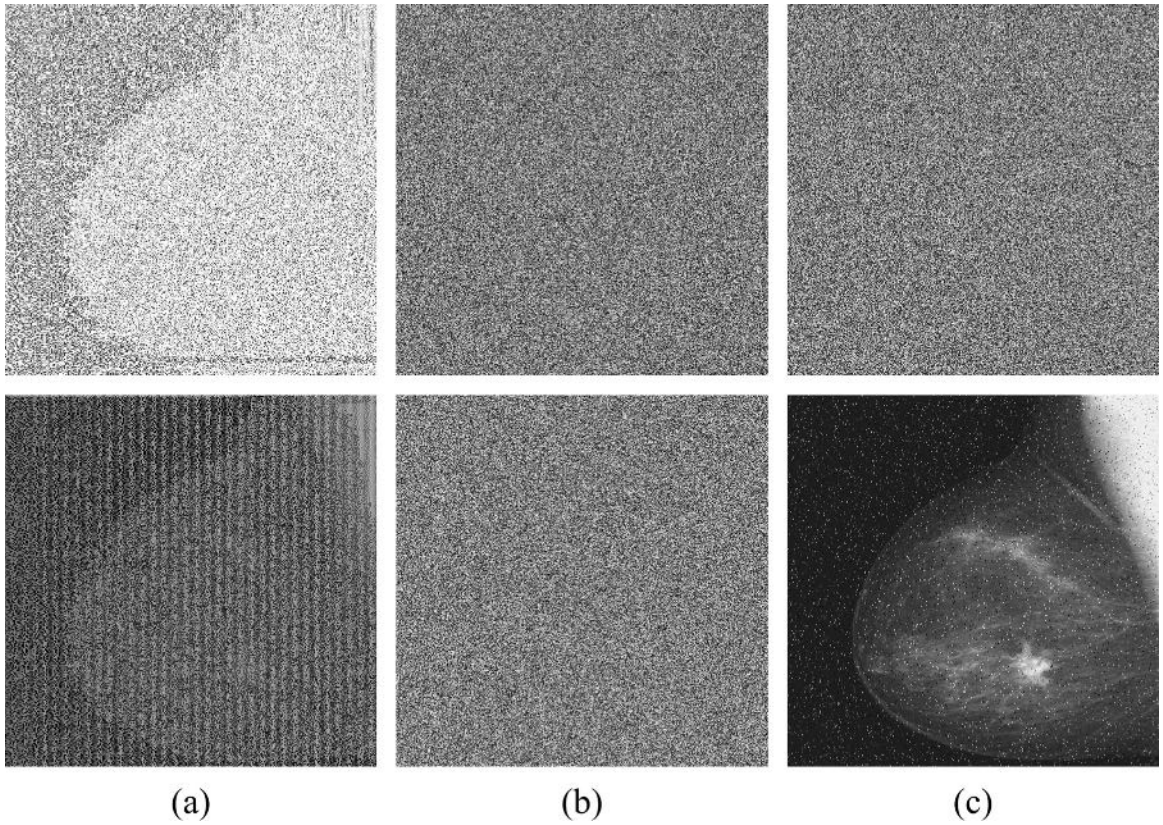

Fig. 15. Noise robustness. (a)–(c) are the cipher-images contaminated with 1% salt & pepper noise, and their reconstructed images based on the schemes of (a) Zhou [33], (b) DecomCrypt [21], and (c) EMMIE.

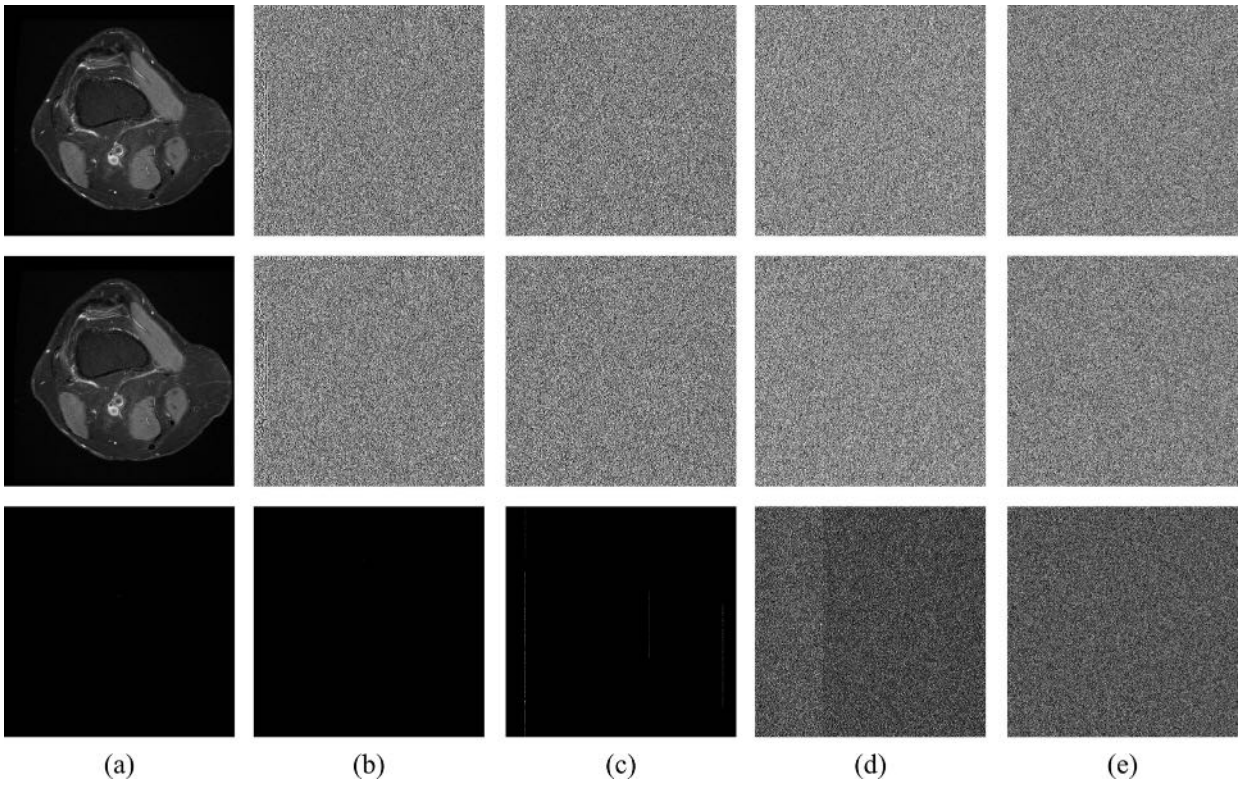

Fig. 16. Differential attack to different algorithms. From top to bottom rows, (a) the original images and their differences, (b)–(d) are the cipher-images and their differences using the (b) Zhou's algorithm in [34], (c) Zhu's algorithm in [33] and (d) DecomCrypt in [21], (e) EMMIE (Sobel, 0.01).

Table 3
NPCR and UACI results of different encryption algorithms.

Image	NPCR				UACI			
	Zhu's	Zhou's	DecomCrypt	EMMIE	Zhu's	Zhou's	DecomCrypt	EMMIE
1	0.0236	0.00001526	0.9692	**0.9966**	0.0078	0.000008557	0.2348	**0.3350**
2	0.0192	0.00001526	0.9757	**0.9958**	0.0066	0.000008557	0.2756	**0.3338**
3	0.0161	0.00001526	0.9780	**0.9960**	0.0053	0.000008557	0.2453	**0.3354**
4	0.0057	0.00001526	0.9509	**0.9955**	0.0018	0.000008557	0.2258	**0.3358**
5	0.0225	0.00001526	0.9474	**0.9963**	0.0078	0.000008557	0.2331	**0.3358**
6	0.0127	0.00001526	0.9415	**0.9955**	0.0043	0.000008557	0.2100	**0.3359**
7	0.0341	0.00001526	0.9397	**0.9959**	0.0116	0.000008557	0.2112	**0.3358**
8	0.0257	0.00001526	0.9581	**0.9965**	0.0086	0.000008557	0.2167	**0.3343**
9	0.0482	0.00001526	0.9675	**0.9962**	0.0164	0.000008557	0.2397	**0.3347**
10	0.0162	0.00001526	0.9291	**0.9957**	0.0053	0.000008557	0.2249	**0.3348**
11	0.0355	0.00001526	0.9692	**0.9960**	0.0120	0.000008557	0.2348	**0.3330**
12	0.0110	0.00001526	0.9011	**0.9955**	0.0036	0.000008557	0.2061	**0.3362**
13	0.0219	0.00001526	0.9531	**0.9958**	0.0075	0.000008557	0.2002	**0.3337**
14	0.0632	0.00001526	0.9152	**0.9961**	0.0216	0.000008557	0.2137	**0.3345**
15	0.0121	0.00001526	0.9085	**0.9956**	0.0041	0.000008557	0.2348	**0.3348**
16	0.0043	0.00001526	0.9347	**0.9963**	0.0014	0.000008557	0.2021	**0.3341**
Average	0.0232	0.00001526	0.9462	**0.9960**	0.0079	0.000008557	0.2256	**0.3348**

changed original images. A slight change in the original image will result in a significant difference in an elaborate encryption method to ensure the cipher-image defect the differential attack. A plain-image of EMMIE is decomposed into several bit-planes and then encrypted to be a cipher-image by the XOR operation and bit-level diffusion process. In the scheme of EMMIE, the cipher-image should be highly sensitive to the change of plain-image due to the influence of bit-level diffusion.

The number of pixel change rate (NPCR) and unified average changing intensity (UACI) are two common methods to quantitatively evaluate the efficiency of an encryption algorithm in defecting the differential attack, which are defined as

$$NPCR = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\mathcal{A}(m,n)}{MN} \times 100\%, \tag{7}$$

$$UACI = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(\frac{|E_1(m,n) - E_2(m,n)|}{G-1}\right) \times 100\%, \tag{8}$$

where G is the gray level of the image; E_1 and E_2 are two $M \times N$ cipher-images and their original images are in one pixel difference. Function $\mathcal{A}(m,n)$ is the number of different pixels between E_1 and E_2.

EMMIE is compared with the image encryption schemes of Zhou, Zhu, and DecomCrypt to asses the performance on withstanding the differential attack. All the parameters and the source image of the

methods are the same as Section 4.2. Two original images with one pixel difference are encrypted by the four algorithms. Their comparison results are shown in Fig. 16. A slight difference in the original image, EMMIE is able to generate a significant change in the encrypted results as shown in Fig. 16(e), which outperforms other three encryption algorithms on defending the differential attack.

In our experiment, 16 test images are selected from the Database of Computer Vision Group in University of Granada.[1] The images are 256× 256 medical images. We use the same parameter setting as shown in Fig. 16. Considering the different image size, we use Fig. 3 (s) as the source image for the DecomCrypt and EMMIE.

Table 3 lists the NPCR and UACI results of four image encryption algorithms. A NPCR value more than 99% possessed, and an UACI obtained near to 33% mean that an image encryption algorithm is secure [37,38]. As can be seen from Table 3, NPCR and UACI values of EMMIE are 99.60% and 33.48% in average. In terms of capability defending differential attack, the measure results further demonstrate that EMMIE is superior to the other three algorithms.

5. Conclusion

A lossless edge maps based image cryptosystem for medical image is proposed, which promotes security efficiency with a machine-friendly binary system. Many kinds of edge maps with various edge detectors can be applied into EMMIE, which can encrypt different types of medical images. The histograms of the cipher-images are approximately flat even with blurry edge maps, which verify EMMIE possessing a strong robustness for fuzzy edge maps by the simulation results. The analysis of security demonstrates EMMIE is a secure algorithm. Source image, edge detector, and the parameters of scrambling method compose the keys of EMMIE and their combinations are significantly large to defend the Bruce-force attack. To further evaluates the security level of EMMIE, as is shown in the comparisons with other state-of-the-art methods, EMMIE possesses a higher pixel correlation, stronger key sensitivity and error robustness, and a better performance against differential attack with less time cost.

Acknowledgment

This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/016/2015/A1 and by the Research Committee at University of Macau under Grants MYRG 2014-00003-FST and MYRG 2016-00123-FST.

References

[1] S. Mitra, B. Uma Shankar, Medical image analysis for cancer management in natural computing framework, Inf. Sci. 306 (2015) 111–131.
[2] A. Phophalia, A. Rajwade, S.K. Mitra, Rough set based image denoising for brain MR images, Signal Process. 103 (2014) 24–35.
[3] Z. Ji, Y. Xia, Q. Sun, G. Cao, Q. Chen, Active contours driven by local likelihood image fitting energy for image segmentation, Inf. Sci. 301 (2015) 285–304.
[4] H. Wu, J. Huang, Y. Shi, A reversible data hiding method with contrast enhancement for medical images, J. Vis. Commun. Image Represent. 31 (2015) 146–153.
[5] H. Jung, K. Sung, K.S. Nayak, E.Y. Kim, J.C. Ye, k-t focuss: a general compressed sensing framework for high resolution dynamic MRI, Magn. Reson. Med. 61 (2009) 103–116.
[6] F. Cao, H.K. Huang, X.Q. Zhou, Medical image security in a HIPAA mandated PACS environment, Comput. Med. Imag. Graph. 27 (2003) 185–196.
[7] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process. 91 (2011) 949–954.
[8] L. Zhang, Z. Zhu, B. Yang, W. Liu, H. Zhu, M. Zou, Cryptanalysis and improvement of an efficient and secure medical image protection scheme, Math. Probl. Eng. 2015 (2015) 11.
[9] L. Zhang, Z. Zhu, B. Yang, W. Liu, H. Zhu, M. Zou, Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach, Math. Probl. Eng. 2015 (2015) 9.
[10] H.-I. Hsiao, J. Lee, Fingerprint image cryptography based on multiple chaotic systems, Signal Process. 113 (2015) 169–181.
[11] H. Cheng, X. Li, Partial encryption of compressed images and videos, IEEE Trans. Signal Process. 48 (2000) 2439–2451.
[12] Y. Sadourny, V. Conan, A proposal for supporting selective encryption in JPSEC, IEEE Trans. Consum. Electron. 49 (2003) 846–849.
[13] Y. Ou, C. Sur, K. Rhee, Region-based selective encryption for medical imaging, in: F. Preparata, Q. Fang (Eds.), Frontiers in Algorithmics, Lecture Notes in Computer Science, vol. 4613, Springer, Berlin, Heidelberg, 2007, pp. 62–73.
[14] G. Alvarez, S. Li, L. Hernandez, Analysis of security problems in a medical image encryption system, Comput. Biol. Med. 37 (2007) 424–427.
[15] K. Martin, R. Lukac, K.N. Plataniotis, Efficient encryption of wavelet-based coded color images, Pattern Recognit. 38 (2005) 1111–1115.
[16] D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, A joint encryption/watermarking system for verifying the reliability of medical images, IEEE Trans. Inf. Technol. Biomed. 16 (2012) 891–899.
[17] D. Bouslimi, G. Coatrieux, C. Roux, A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images, Comput. Methods Progr. Biomed. 106 (2012) 47–54.
[18] B. Bakhache, J.M. Ghazal, S. El Assad, Improvement of the security of ZigBee by a new chaotic algorithm, IEEE Syst. J. 8 (2014) 1021–1030.
[19] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image Vis. Comput. 27 (9) (2009) 1371–1381.
[20] C. Li, Y. Liu, T. Xie, M.Z.Q. Chen, Breaking a novel image encryption scheme based on improved hyperchaotic sequences, Nonlinear Dyn. 73 (3) (2013) 2083–2089.
[21] Y. Zhou, W. Cao, C.L.P. Chen, Image encryption using binary bitplane, Signal Process. 100 (2014) 197–207.
[22] C. Li, Cracking a hierarchical chaotic image encryption algorithm based on permutation, Signal Process. 118 (2016) 203–210.
[23] R.C. Gonzalez, R.E. Woods, Digital Image Processing, 3rd edition, Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2006.
[24] M. Setayesh, M. Zhang, M. Johnston, A novel particle swarm optimisation approach to detecting continuous, thin and smooth edges in noisy images, Inf. Sci. 246 (2013) 28–51.
[25] H. Greenspan, C.H. Anderson, S. Akber, Image enhancement by nonlinear extrapolation in frequency space, IEEE Trans. Image Process. 9 (2000) 1035–1048.
[26] J. Huang, X. You, Y.Y. Tang, L. Du, Y. Yuan, A novel iris segmentation using radial-suppression edge detection, Signal Process. 89 (2009) 2630–2643.
[27] V. Madisetti, D. Williams, The Digital Signal Processing Handbook, CRC Press, Boca Raton, FL USA, 2010.
[28] M. Jacob, M. Unser, Design of steerable filters for feature detection using canny-like criteria, IEEE Trans. Pattern Anal. Mach. Intell. 26 (2004) 1007–1019.
[29] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, Image encryption using P-Fibonacci transform and decomposition, Opt. Commun. 285 (2012) 594–608.
[30] Y. Zhou, Z. Hua, C.-M. Pun, C.L.P. Chen, Cascade chaotic system with applications, IEEE Trans. Cybern. 45 (2015) 2001–2012.
[31] Y. Zhou, L. Bao, C.L.P. Chen, Image encryption using a new parametric switching chaotic system, Signal Process. 93 (2013) 3039–3052.
[32] Z. Hua, Y. Zhou, Image encryption using 2D logistic-adjusted-sine map, Inf. Sci. 339 (2016) 237–253.
[33] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, (n, k, p)-gray code for image systems, IEEE Trans. Cybern. 43 (2013) 515–529.
[34] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (2011) 1171–1186.
[35] Z. Hua, Y. Zhou, C.-M. Pun, C.L.P. Chen, 2d sine logistic modulation map for image encryption, Inf. Sci. 297 (2015) 80–94.
[36] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, Inf. Sci. 264 (2014) 317–339.
[37] Y. Wu, J.P. Noonan, S. Agaian, NPCR and UACI randomness tests for image encryption, J. Sel. Areas Telecommun. (2011) 31–38.
[38] O.S. Faragallah, Efficient confusion-diffusion chaotic image cryptosystem using enhanced standard map, Signal Image Video Process. (2014) 1–10.

[1] http://decsai.ugr.es/cvg/dbimagenes/gbio256.php