31st Annual International Conference of the IEEE EMBS
Minneapolis, Minnesota, USA, September 2-6, 2009

A Lossless Encryption Method for Medical Images Using Edge Maps

Yicong Zhou, *Member, IEEE*, Karen Panetta, *Fellow, IEEE*, and Sos Agaian, *Senior Member, IEEE*

***Abstract*—Image encryption is an effective approach for providing security and privacy protection for medical images. This paper introduces a new lossless approach, called EdgeCrypt, to encrypt medical images using the information contained within an edge map. The algorithm can fully protect the selected objects/regions within medical images or the entire medical images. It can also encrypt other types of images such as grayscale images or color images. The algorithm can be used for privacy protection in the real-time medical applications such as wireless medical networking and mobile medical services.**

I. Introduction

MEDICAL images are generated by using different technologies of medical imaging for many clinical applications to diagnose or examine diseases. These technologies include radiography, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Photoacoustic imaging, and many others. Medical images may contain a large amount of private and important information about patients. Some of them may be included in a patient's medical record along with text based personal information, clinical diagnosis and examination records. They may be archived as digital formats in the computer or transmitted among hospitals or doctors for various clinical services. Some rapidly growing new clinical services such as telemedicine and e-health transmit medical information over telephone or networks. Providing security of medical images becomes an important issue for hospitals and medical service organizations. Image encryption is an effective method to secure medical images while preserving their integrity.

Many approaches for medical image encryption have been developed in recent years. For example, medical images can be encrypted by combining different techniques such as pixel arrangement and chaotic maps [1], or AES and chaotic maps [2]. Nevertheless, these methods suffer from either high computational costs or low level of security due to leakage of original image information. Recently, a technique to encrypt interleaved patient information in medical images has been designed to reduce storage and transmission overhead [3, 4]. However, this method only protects text based patient information.

Encryption methods for medical images in the compression domain are mainly based on selective encryption such as the concept of the Advanced Encryption Standard (AES) to encrypt the selective JPEG2000 bitstream [5], Region of Interest (ROI) [6], or sensitive precincts within medical images [7]. Different from other visual data, medical images may contain some important visual information of diseases or afflictions to the human body. Thus, the encryption schemes in the compression domain may not be suitable for protecting medical images because lossy compression processes may lose some image data which may cause some negative misdiagnosis. Therefore, non-compression methods or lossless techniques are desirable.

The edge map is generally used in image enhancement, compression, segmentation and recognition. In this paper, we investigate a new application of the edge map for medical image encryption in the non-compression domain. We introduce a new medical image encryption algorithm using an edge map, called EdgeCrypt. The algorithm encrypts medical images by changing image data without compressing images, preserving the quality of medical images.

The rest of the paper is organized as follow. Section II introduces the EdgeCrypt algorithm. Experimental examples and analysis are addressed in Section III to show the performance of the EdgeCrypt algorithm for medical image encryption. A cryptanalysis is addressed in Section IV. Section V discusses the conclusion.

II. The Medical Image Encryption Algorithm

In this section, we introduce a new algorithm, EdgeCrypt, to encrypt medical images using an edge map.

The underlying foundation of the EdgeCrypt algorithm is to encrypt medical images via changing image data. It obtains the edge map of the medical image by applying a specific type of edge detector such as Canny, or Sobel, or Prewitt, or any other, with a certain threshold value. The algorithm then decomposes the medical image into several binary bit planes, encrypts all bit planes by performing an XOR operation between the edge map and each bit plane, encrypts the edge map using a random bit sequence generated from the logic chaotic map, interleaves the encrypted edge map among the XORed bit planes, reverses the order of all bit planes, and combines them to obtain the final encrypted medical images. The block diagram of the EdgeCrypt algorithm is shown in Fig. 1.

To improve the security of the algorithm, a bit-plane shuffling process is added to change the values of image pixels in the vertical direction. The users have flexibility to utilize any existing approach to shuffle the order of bit planes. We simply reverse the order of the bit planes in this paper.

Yicong Zhou and Karen Panetta are with Department of Electrical and Computer Engineering, Tufts University, Medford, MA 02155, USA (YZ phone: 617-627-5183; fax: 617-627-3220; e-mail: yzhou0a@ece.tufts.edu; KP e-mail: karen@ece.tufts.edu).

Sos Agaian is with Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249, USA (e-mail: Sos.Agaian@utsa.edu).

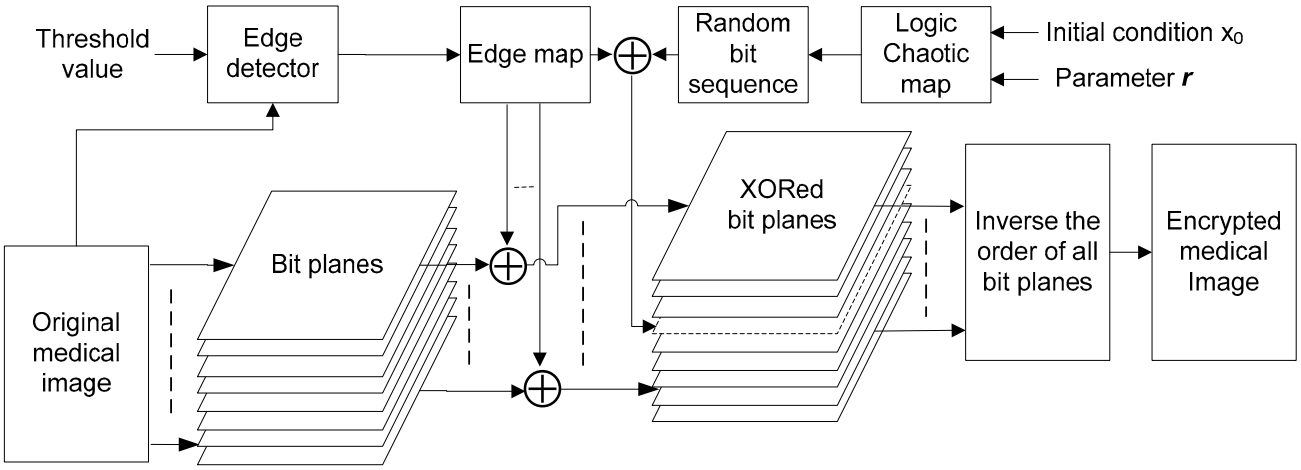

Fig. 1. The block diagram of the EdgeCrypt algorithm.

A random bit sequence generated from a logic chaotic map is used to encrypt the edge map. The encrypted edge map is obtained by performing an additional XOR operation between each bit of a random bit sequence and each pixel of the edge map. It is then interleaved among the XORed bit planes. The logic chaotic map is defined as follow.

$$x_{n+1} = r x_n (1 - x_n) \tag{1}$$

where parameter r is a rational number, $3.5699456 < r \le 4$, $0 < x_n < 1$ and $n = 0, 1, 2, ...$

If the size of the edge map is $M \times N$, the random bit sequence can be generated by the definition,

$$b_n = \begin{cases} 1 & x_n \ge 0.5 \\ 0 & x_n < 0.5 \end{cases} \tag{2}$$

where $n = 0, 1, 2, ..., MN - 1$.

The security keys for the EdgeCrypt algorithm include the initial condition x_0 and parameter r of the logic chaotic map, the interleaved location of the edge map, the type of the edge detector and its threshold value. The users have flexibility to choose any existing approach for edge detection and select any threshold value for the edge detector. The edge map can also be interleaved between any two bit planes.

In the decryption process, the authorized users do not have to know the type of the edge detector and its threshold value to reconstruct the original image because the edge map has been sent to users along with the encrypted image. However, the edge map can be completely recovered only by using the correct security keys: the location to interleave the edge map as well as the initial condition x_0 and parameter r of the logic chaotic map.

The decryption process first decomposes the encrypted image into binary bit planes. It then reverses the order of all bit planes and extracts the edge map from the bit planes. The edge map is reconstructed using security keys. The algorithm performs an XOR operation between the edge map and each bit plane and combines the XORed bit planes to obtain the reconstructed medical image.

III. Experimental Results and Analysis

The EdgeCrypt algorithm has been successfully implemented in more than 16 medical images. Some simulation examples are presented in this section to show the performance of the algorithm for medical image encryption. A comparison is made with the AES algorithm to show the encryption efficiency of the EdgeCrypt algorithm. The algorithm is also proved to be able to encrypt the selective objects /regions and other types of images.

The interleaved location of the edge map in all examples in this section is the between the first bit plane, which contains the most significant bits of all image pixels, and the second bit plane which contains the second most significant bits of image pixels.

A. Examples of Medical Image Encryption

Fig.2 gives an example of the MRI image encryption. The encrypted image in Fig.2 (c) is completely different from the original MRI brain image in Fig.2 (a). The histogram in Fig.2 (g) shows the nearly equal distribution of the pixel values in encrypted image. This makes the encrypted image difficult to be broken by attacks. The original image can be protected with high level of security. This is one of advantages of the presented algorithm.

The original image has been completely reconstructed. The reconstruction can be verified from the reconstructed image in Fig.2(d) and its histogram in Fig.2(h) because both of them are exactly the same as the original image.

The edge map in this example is generated by the Sobel edge detector with threshold 0.5. It is encrypted by logic chaotic map with the initial condition $x_0 = 0.6$ and the parameter $r = 3.65$.

An example of the CT image encryption is shown in Fig.3. The original CT image has been fully encrypted (Fig.3 (c)) and completely reconstructed (Fig.3 (d)). This perfect reconstruction is also evident via the histogram of the

difference between the original image and the reconstructed image because the difference between them is zero. These results show that the EdgeCrypt algorithm is a lossless encryption method and it can fully encrypt the medical images.

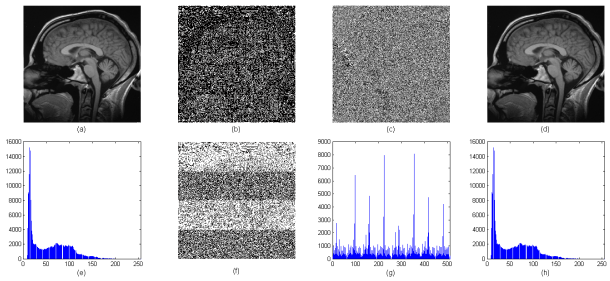

Fig. 2. MRI image encryption. (a) The original MRI image; (b) The edge map obtained by Sobel edge detector with threshold 0.5; (c) The encrypted MRI image, (d) The reconstructed MRI image; (e) Histogram of the original MRI image; (f) The encrypted edge map, $x_0 = 0.6,\ r = 3.65$; (g) Histogram of the encrypted MRI image; (h) Histogram of the reconstructed MRI image.

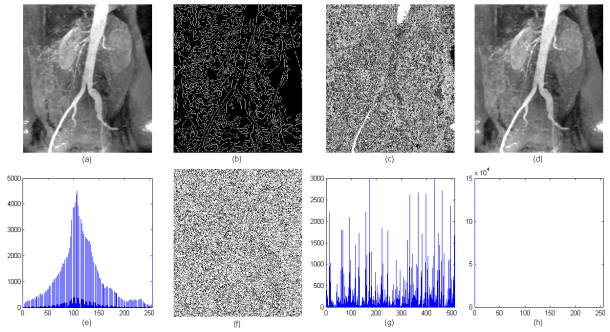

Fig. 3. CT image encryption. (a) The original CT image; (b) The edge map obtained by Canny edge detector with threshold 0.1; (c) The encrypted CT image, (d) The reconstructed CT image; (e) Histogram of the original CT image; (f) the encrypted edge map, $x_0 = 0.2,\ r = 3.8$; (g) Histogram of the encrypted CT image; (h) Histogram of the difference between (a) and (d).

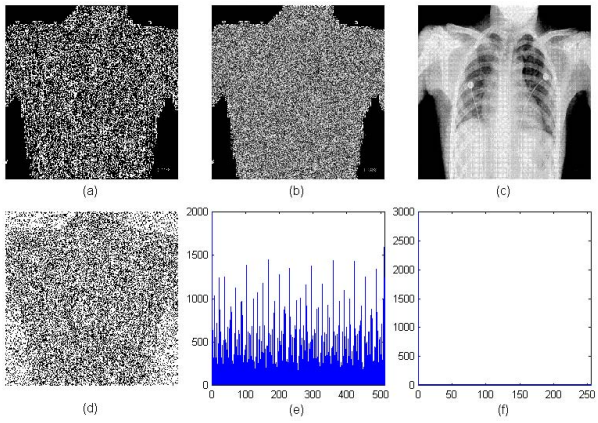

Fig. 4. X-ray image encryption. (a) The edge map obtained by Prewitt edge detector with threshold 0.3; (b) The encrypted X-ray image; (c) The reconstructed X-ray image; (d) the encrypted edge map, $x_0 = 0.8$, $r = 3.7$; (e) Histogram of the encrypted X-ray image; (f) Histogram of the difference between the original X-ray image and the reconstructed image.

The edge map in this example is obtained from the Canny edge detector with threshold 0.1. It is also protected by the logic chaotic map with security keys, $x_0 = 0.2$ and $r = 3.8$.

An example of X-ray image encryption is shown in Fig. 4. The edge map in this example is obtained by the Prewitt edge detector with threshold 0.3. It is encrypted by logic chaotic map with security keys, $x_0 = 0.8$ and $r = 3.7$.

The interesting result is the encrypted image in Fig.4 (b). It shows that the EdgeCrypt algorithm can be used to protect the selected objects or regions within medical images which may contain important or private information of the patients. This is another advantage of the algorithm.

The original X-ray image is also completely reconstructed in Fig. 4(c) because the histogram of the difference between the reconstructed X-ray image and the original X-ray image is zero in Fig.4 (f). These results further verify the EdgeCrypt algorithm is a lossless encryption method.

B. Performance Measure and Comparison

To show the efficiency of the EdgeCrypt algorithm for medical image encryption, it was compared with the AES algorithm implemented in [8] over several images.

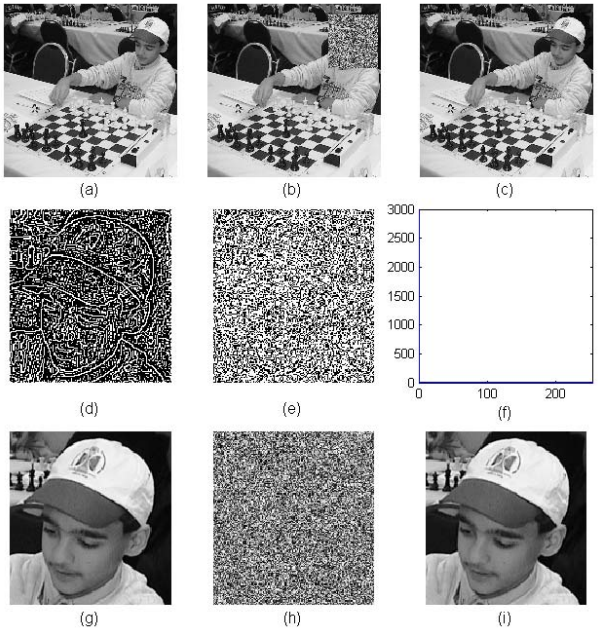

Fig. 5. Grayscale image encryption. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) The edge map obtained by Roberts edge detector with threshold 0.4; (e) The encrypted edge map, $x_0 = 0.8$, $r = 3.7$; (f) Histogram of the difference between the original image and the reconstructed image. (g) Selected object; (h) Encrypted object; (i) Reconstructed object.

The 512×512 MRI brain image shown in Fig. 1(a) is used as an example of the obtained results. The execution time of this MRI image encryption using the EdgeCrypt algorithm and then the AES algorithm is measured in a computer working Windows XP operation system with 2GB memory and CPU using Intel Core2 Quad Q6700. The AES algorithm takes 521.67 seconds to encrypt this MRI image. However, the EdgeCrypt algorithm spends only 17.78 second to encrypt the same MRI image. This shows that the speed of the EdgeCrypt algorithm is much faster than that of the AES

algorithm. This shows the suitability of the EdgeCrypt algorithm for real-time medical applications such as wireless medical networking and mobile medical services.

Furthermore, The EdgeCrypt algorithm is easy to implement in hardware such as an FPGA since all its processes operate on the binary bit levels.

C. Other applications

In addition, the EdgeCrypt algorithm is able to encrypt other types of images such as grayscale images or color images.

Fig.5 provides an example of grayscale image encryption. This example shows that the EdgeCrypt algorithm can be used for ensuring the security of grayscale images. It further demonstrates that the algorithm can encrypt the selected regions or objects in images for private protection.

IV. Cryptanalysis

Security is important not only for the encrypted objects but also for the encryption algorithm itself. We will discuss the security issues of the EdgeCrypt algorithm in this section.

A. Security Key Space

The security keys of the EdgeCrypt algorithm consist of the location to interleave the edge map, the type of the edge detector and its threshold, as well as the initial condition and the parameter of the logic chaotic map. A large number of possible types of edges detectors can be used for the EdgeCrypt algorithm. The possible threshold values for a specific edge detector are unlimited. The initial condition x_0 and the parameter r of the logic chaotic map also have an infinite number of possible choices. As a result, the possible number of combinations of these security keys becomes inexhaustible. Hence, the security key space of the EdgeCrypt algorithm is unlimited.

B. Plaintext Attacks

An edge map is determined by the type of the edge detector, the threshold of the edge detector and the content of the original image. The pixel data of the encrypted bit-planes changes with different edge detectors and the original image data.

The edge map is encrypted by a pseudo-random bit sequence generated by the logic chaotic map. This ensures that the edge map as one of security keys for the EdgeCrypt algorithm to be well protected. It is then interleaved into the encrypted bit planes. The order of all bit planes is the reversed. The resulting encrypted image is the combination of all of them. These processes further change the image pixel data and result the nearly equal distribution of the pixel values of the encrypted image. Thus, the data of the encrypted image are immune to plaintext attacks such as the known-plaintext attack and chosen-plaintext attack. This allows encrypted medical images to be protected with a high level of security.

V. Conclusion

In this paper, we have introduced a new algorithm for medical image encryption which uses the edge map. The algorithm encrypts medical images by combining four different processes to change image data. The nearly equal data distribution of the encrypted medical image has been obtained after several encryption processes.

The users have flexibility to choose any existing edge detector and its threshold values for the EdgeCrypt algorithm or interleave the edge map between any two bit planes. The security keys of the EdgeCrypt algorithm have an infinite number of possible combinations. This ensures the unauthorized users have difficulty to decode the encrypted medical images. Thus, original medical images are protected with a high level of security.

Experimental examples have demonstrated that the EdgeCrypt algorithm is a lossless encryption method and can fully encrypt selected objects or regions within the medical images or entire medical images. The EdgeCrypt algorithm can be used for real-time medical applications such as wireless medical networking and mobile medical services. It can overcome the plaintext attacks.

References

[1] K. Usman, H. Juzoji, I. Nakajima, S. Soegidjoko, M. Ramdhani, T. Hori, and S. Igi, "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security," in e-Health Networking, Application and Services, 2007 9th International Conference on, 2007, pp. 244-247.

[2] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography," in Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on, 2008, pp. 1-5.

[3] R. Acharya U, P. Subbanna Bhat, S. Kumar, and L. C. Min, "Transmission and storage of medical images with patient information," Computers in Biology and Medicine, vol. 33, no. 4, pp. 303-310, 2003.

[4] G. Alvarez, S. Li, and L. Hernandez, "Analysis of security problems in a medical image encryption system," Computers in Biology and Medicine, vol. 37, no. 3, pp. 424-427, 2007.

[5] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt, and A. Uhl, "Confidential storage and transmission of medical image data," Computers in Biology and Medicine, vol. 33, no. 3, pp. 277-292, 2003.

[6] Y. Ou, C. Sur, and K. Rhee, "Region-Based Selective Encryption for Medical Imaging," in Frontiers in Algorithmics, 2007, pp. 62-73.

[7] Z. Brahimi, H. Bessalah, A. Tarabet, and M. K. Kholladi, "A new selective encryption technique of JPEG2000 codestream for medical images transmission," in Systems, Signals and Devices, 2008. IEEE SSD 2008. 5th International Multi-Conference on, 2008, pp. 1-4.

[8] J. J. Buchholz, "Matlab Implementation of the Advanced Encryption Standard," http://buchholz.hs-bremen.de/aes/aes.htm, 2001.