ELSEVIER
SIGNAL
PROCESSING
An International Journal
A publication of the European Association for Signal Processing (EURASIP)
EURASIP

www.elsevier.com/locate/sigpro

Medical Image Encryption Using Edge Maps

Weijia Cao, Yicong Zhou, C.L. Philip Chen, Liming Xia

PII: S0165-1684(16)30266-3
DOI: http://dx.doi.org/10.1016/j.sigpro.2016.10.003
Reference: SIGPRO6278

To appear in: *Signal Processing*

Received date: 2 March 2016
Revised date: 22 September 2016
Accepted date: 3 October 2016

Cite this article as: Weijia Cao, Yicong Zhou, C.L. Philip Chen and Liming Xia Medical Image Encryption Using Edge Maps, *Signal Processing* http://dx.doi.org/10.1016/j.sigpro.2016.10.003

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*

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.

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

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, 7, 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, 12, 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, 19, 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

[*] Corresponding author. Tel.: +853 88228458; Fax: +853 88222426
Email address: yicongzhou@umac.mo (Yicong Zhou)