Computers in Biology and Medicine 43 (2013) 1000–1010

Contents lists available at SciVerse ScienceDirect

Computers in Biology and Medicine

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

An efficient and secure medical image protection scheme based on chaotic maps

Chong Fu [a,*], Wei-hong Meng [b], Yong-feng Zhan [b], Zhi-liang Zhu [c], Francis C.M. Lau [d], Chi K. Tse [d], Hong-feng Ma [e]

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Northern Hospital, Shenyang 110016, China
[c] Software College, Northeastern University, Shenyang 110004, China
[d] Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Hunghom, Hong Kong
[e] TeraRecon, 4000 East 3rd Avenue, Suite 200, Foster City, CA 94404, United States

ARTICLE INFO

Article history:
Received 3 May 2011
Accepted 7 May 2013

Keywords:
Medical image protection
Chaos
Permutation–substitution
Arnold cat map
PACS

ABSTRACT

Recently, the increasing demand for telemedicine services has raised interest in the use of medical image protection technology. Conventional block ciphers are poorly suited to image protection due to the size of image data and increasing demand for real-time teleradiology and other online telehealth applications. To meet this challenge, this paper presents a novel chaos-based medical image encryption scheme. To address the efficiency problem encountered by many existing permutation–substitution type image ciphers, the proposed scheme introduces a substitution mechanism in the permutation process through a bit-level shuffling algorithm. As the pixel value mixing effect is contributed by both the improved permutation process and the original substitution process, the same level of security can be achieved in a fewer number of overall rounds. The results indicate that the proposed approach provides an efficient method for real-time secure medical image transmission over public networks.

1. Introduction

With the advancement of digital technologies, an overwhelming majority of medical images now exist in electronic format for easy storage, maintenance, and retrieval. Computer networks make it very convenient to access and share data among medical personnel, leading to improvement in the quality of patient care. Medical applications often deal with patients' data that are private and should only be accessible to authorized staff. Consequently, an important issue is how to effectively protect the confidentiality of patients' information stored as well as of those of any kind transmitted for legal and ethical reasons [1–6]. Picture Archiving and Communication Systems (PACS) as well as Digital Imaging and Communications in Medicine (DICOM) provide the current medical image transport and storage standards [7]. Delivery of image data in a PACS environment is usually over a hospital intranet that can be protected by a firewall or proxy from unauthorized intrusions. However, for telemedicine applications, as the images are transmitted over the Internet and even through wireless networks, there is a potential threat to patient's privacy. Therefore, guidelines and mandates for ensuring medical image security have been issued by several major medical imaging communities such as American College of Radiology (ACR) and Society of Computer Applications in Radiology (SCAR). Moreover, the Health Insurance Portability and Accountability Act (HIPAA), enacted by the United States Congress and signed by President Bill Clinton in 1996, obliges health care institutions to take proper measures to ensure that patients' information is only accessible to people who have a professional need [8].

Security mechanisms deployed in existing digital medical image systems are almost exclusively based on the conventional block ciphers such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and International Data Encryption Algorithm (IDEA). However, due to the size of image data and increasing demand for real-time teleradiology and other online telehealth applications, these conventional encryption algorithms are not suitable for practical image encryption, as they introduce delay. To meet this challenge, a variety of image encryption schemes has been proposed. Among them, chaos-based algorithms have offered a good trade-off between security and performance. Since the 1990s, many researchers have noticed that there exists tight relationship between chaos and cryptography. The intrinsic properties of chaotic dynamical systems such as extreme sensitivity to initial conditions and system parameters, ergodicity and mixing property naturally satisfy the essential design principles of a cryptosystem such as avalanche, confusion and diffusion. Recently, there has been extensive research on chaos-based image

* Corresponding author. Tel.: +86 24 83688871, +86 24 23388825.
E-mail addresses: fuchong@ise.neu.edu.cn, fuchong75@hotmail.com (C. Fu).

0010-4825/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.compbiomed.2013.05.005

cryptosystems [9–42]. A brief overview of some major contributions is given below.

In [9], Fridrich suggested a chaos-based image encryption scheme comprising of two modules: chaotic confusion and pixel diffusion. The former permutes the pixels of a plain image with an invertible 2D chaotic map while the latter alters the pixel values sequentially by using a chaotic key stream. This architecture, known as confusion–diffusion or permutation–substitution, is the first general architecture which guides the design of chaos-based image cipher. In [10], Scharinger proposed a fast image encryption algorithm. In his scheme, chaotic Kolmogorov flow and a shift-registered pseudo-random number generator are employed to eliminate the strong correlation among adjacent pixels and confuse the relationship between cipher image and plain image. In [12,13], the 2D chaotic cat map and baker map are generalized to 3D to enhance the effectiveness of pixel permutation. It can be seen that these two improved chaotic maps can perform the operation of shuffling the pixel positions in a more efficient manner than 2D-based methods. In [16], Belkhouche et al. proposed a novel permutation method based on chaotic sequence sorting rather than conventional 2D chaotic maps, so as to address the drawback of periodicity of some discretized version chaotic maps. In [17], a symmetric block cipher based on the improved standard map has been designed and presented for encrypting large-volume data sets. In this approach, the computational complexity for the permutation mode is significantly reduced by introducing of a sine table. In [22], Xiang et al. proposed a selective image encryption scheme, which only ciphers a portion of significant bits of each pixel by the key-stream generated from a one-way coupled map lattice. It is reported that an acceptable level of security can be achieved by only encrypting the higher 4 bits of each pixel, and therefore the encryption time is substantially reduced. In [24], a way of improving the security of chaos-based cryptosystem is proposed, using a hierarchy of one dimensional chaotic maps and their coupling, which can be viewed as a high dimensional dynamical system. In [26,27], Gao et al. reported two chaos-based image encryption schemes, which employ an image total shuffling matrix to shuffle the positions of image pixels and use a hyper-chaotic system to confuse the relationship between the plain image and the cipher-image, respectively. In [28], Wong et al. suggested to introduce certain diffusion effect in the confusion stage by simple sequential add-and-shift operations. The purpose is to reduce the workload of the time-consuming diffusion part so that fewer overall rounds and hence a shorter encryption time is needed. To overcome the drawbacks of small key space and weak security in the widely used one-dimensional chaotic system, Sun et al. [29] proposed a spatial chaos map based image encryption scheme. The basic idea is to encrypt the image in space with spatial chaos map pixel-by-pixel, and then the pixels are confused in multiple directions of space. In [32], Patidar et al. proposed a symmetric image cryptosystem which comprises four encryption rounds. Chaotic standard and logistic maps are employed for confusion and diffusion, which are both performed two rounds. In [34], Rhouma et al. presented a one-way coupled map lattice (OCML) based color image encryption scheme. To enhance the cryptosystem security, a 192-bit-long external key is used to generate the initial conditions and the parameters of the OCML by making some algebraic transformations to the secret keys. In [37], Wong et al. proposed a more efficient diffusion mechanism using simple table lookup and swapping techniques as a light-weight replacement of the 1D chaotic map iteration. They reported that at a similar security level, the proposed cryptosystem needs about one-third the encryption time of a similar cryptosystem. In [40], Elashry et al. proposed a homomorphic image cryptosystem with the idea of encrypting the reflectance component after the homomorphic transform and embedding the illumination component as a least significant bit watermark into the encrypted reflectance component. In [41], Borujeni et al. proposed a permutation scheme using the Tompkins–Paige algorithm, which is controlled by pseudorandom parameters generated by a logistic map.

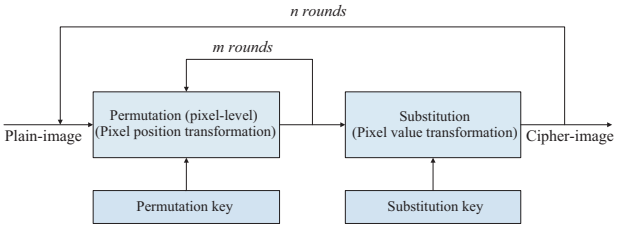

Fig. 1. Common architecture for chaos-based image cipher.

A new approach is suggested in this paper for efficient and secure medical image protection. To improve the efficiency of the chaos-based image cryptosystem, we propose a novel bit-level shuffling algorithm, which introduces a certain substitution mechanism in permutation process. As a result, the same level of security can be achieved in fewer overall encryption rounds as the pixel value mixing effect is contributed by both substitution process and the new permutation process. Performance test results have shown that the proposed medical image cryptosystem is much more efficient than the well-known DES scheme, which renders it a suitable candidate for medical image protection in real-time environments. The rest of this paper is organized as follows. Section 2 presents the architecture of the proposed medical image cryptosystem. The detailed bit-level permutation and substitution algorithms are discussed in Sections 3 and 4, respectively. In Section 5, the security and performance of the proposed medical image cryptosystem are analyzed in detail. Finally, Section 6 concludes the paper.

2. Architecture of the medical image cryptosystem

Permutation–substitution, the most commonly employed architecture in chaos-based image cryptosystem, is illustrated by Fig. 1.

As can be seen from Fig. 1, there are two iterative stages in this architecture. In the permutation stage, the pixels of a plain image are rearranged in a different and usually quite complex order but the pixels themselves are left unchanged. Three two-dimensional area-preserving chaotic maps, Arnold cat map, baker map and standard map, are usually employed to meet this requirement. In the substitution stage, the pixel values are altered sequentially and the modification made to a particular pixel usually depends on the accumulated effect of all the previous pixel values, and therefore the influence of a single pixel can be effectively diffused to the whole cipher-image with several overall rounds encryption. Various discrete and continuous chaotic systems such as logistic map, tent map or Lorenz system can be utilized to calculate a pseudorandom key stream for substitution. Several simple mathematical operations such as XOR, XNOR, shift, add and subtract or their combinations are usually employed to achieve this purpose. To sufficiently eliminate the correlation among adjacent pixels, the permutation operation is usually iterated m ($m \geq 1$) times. Similarly, the whole permutation–substitution operation iterates n ($n \geq 1$) rounds so as to achieve a satisfactory level of security. The initial parameters and conditions of the employed chaotic systems serve as the secret key.

Traditionally, the permutation and substitution are two independent stages. It is well known that the permutation module is weak against many of the common attacks, especially statistical attacks and known/chosen plaintext attacks as the permutation process only shuffles the pixel positions while without pixel value