Commun Nonlinear Sci Numer Simulat 24 (2015) 98–116

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

An efficient and robust image encryption scheme for medical applications

A. Kanso *, M. Ghebleh

Department of Mathematics, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait

ARTICLE INFO

Article history:
Received 3 July 2014
Received in revised form 24 November 2014
Accepted 12 December 2014
Available online 5 January 2015

Keywords:
Cryptography
Chaos
Digital medical image encryption
Selective encryption
Pseudorandom numbers
Cat map

ABSTRACT

In this paper, we propose a novel full and selective chaos-based image encryption scheme suitable for medical image encryption applications. The proposed approach consists of several rounds, where each round is made up of two phases, a shuffling phase and a masking phase. Both phases are block-based and use chaotic cat maps to shuffle and mask an input image. To improve the speed of the proposed scheme while maintaining a high level of security, the scheme employs a pseudorandom matrix, of the same size as the input image, in the masking phase of each round. Blocks of this pseudorandom matrix are permuted in each round of the shuffling phase according to the outputs of some chaotic maps. The proposed scheme applies mixing between blocks of the image in order to prevent cryptanalytic attacks such as differential attacks. Simulation results demonstrate high performance of the proposed scheme and show its robustness against cryptanalytic attacks, thus confirming its suitability for real-time secure image communication.

1. Introduction

Digital medical images are important diagnostic tools. They are generated using a number of technologies and are mainly used for treating and predicting disease. These technologies include X-ray radiography, ultrasound, magnetic resonance imaging (MRI), etc. There exist a number of applications which require storing and transmitting medical images across public channels such as the Internet, and hence making them vulnerable to security threats. Therefore, there is a great need for protecting patient's digital medical images. Cryptography is a field of mathematics and computer science which provides a number of security services. These services include the protection, via a suitable encryption scheme, of private information from being accessed by an unauthorized party. A number of conventional encryption schemes have appeared in the literature such as the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), the Advanced Encryption Standard (AES), etc. [1]. However, these schemes require a large computational time, and are mainly used to protect textual data. Thus, they are not suitable for encrypting digital medical images due the intrinsic characteristics of these images such as (i) large data size, (ii) existence of bulk data capacity, (iii) high redundancy and (iv) strong correlation between adjacent pixels. Nonetheless, a number of approaches based on conventional encryption schemes such as AES have been proposed to protect medical records in the DICOM system [2] and in many other research papers [3–5]. Due to the close relation between chaos theory and cryptography, many chaos-based image encryption schemes have been developed in the

* Corresponding author. Tel.: +965 24985345.
E-mail addresses: akanso@sci.kuniv.edu.kw (A. Kanso), mamad@sci.kuniv.edu.kw (M. Ghebleh).

http://dx.doi.org/10.1016/j.cnsns.2014.12.005
1007-5704/© 2014 Elsevier B.V. All rights reserved.

last two decades [6–23]. However, some of these approaches have security weaknesses or they require a large computational time [24–33].

In recent years, selective image encryption, which is a trend to minimize the processing time for encryption and decryption of images while maintaining a sufficient security level, has grasped the attention of many scientists and engineers who have proposed a number of encryption schemes [5,7,34–41]. Unlike conventional encryption schemes that act on the whole plain image, selective encryption schemes act on selected portions of the plain image. Hence, they can be useful in many real-time medical applications to protect medical records including wireless medical networking and mobile medical services [7]. There exist a number of selection techniques such as edge maps [7], region of interest (ROI) [37] and entropy-based techniques [4].

We propose in this paper an image encryption scheme suitable for full and selective encryption applications, in particular for medical image encryption. Depending on the application, this scheme can be used for encrypting (i) the full plain image or (ii) part of the plain image containing significant information (in which case the insignificant parts are left unencrypted, or encrypted using a lighter encryption method). The significant regions in an image can be identified using a statistical approach (which we describe later). The proposed scheme is based on chaotic cat maps, and hence it inherits the characteristics of such maps including high sensitive dependence on initial conditions and control parameters, random-like behavior, unpredictability, etc. Following our approach in [42], the suggested scheme is composed of several rounds, where each round consists of two phases, a shuffling phase and a masking phase. In the shuffling phase, blocks of the sub-image (the full image in case of full encryption and the significant information in case of selective encryption) and a matrix of pseudorandom numbers of integers as large as the sub-image are shuffled according to iterations of a coupling of chaotic cat maps. In the masking phase, we mask the shuffled sub-image blocks with blocks of the shuffled matrix of pseudorandom numbers. We further apply a mixing approach between the blocks to prevent cryptanalytic attacks such as differential attacks. This technique is shown to speed up the performance of the encryption scheme while maintaining a high level of security. Simulation results are provided to demonstrate the high performance of the proposed scheme. We further show that the scheme is robust against existing attacks.

The paper is organized as follows: Section 2 describes the statistical approach for selection of the ROI. Section 3 gives a detailed description of the proposed image encryption scheme. In Section 4, we study the efficiency of the proposed scheme. In Section 5, we present simulation results to demonstrate the robustness of the suggested scheme against cryptanalytic attacks. Section 6 presents experimental results that show the high security and speed performance of the proposed scheme. We end the paper with some concluding remarks in Sections 7 and 8.

2. Block-based selective encryption

The suggested image encryption scheme can be applied to any digital image as demonstrated in Section 5. However, since medical images possess special features, they are of special interest. Medical images usually consist of two regions (i) the region of interest (ROI) which contains the significant information and (ii) the region of background (ROB) which contains the insignificant information. In this research, we present a new approach to locate the significant information of a given image. In this approach, we divide the matrix representing the input image into square blocks. By omitting a few rows and columns of the plain medical image, if necessary, we assume that the height and width of the image are divisible by the block size. We then use a statistical measure on each block to determine whether it is to be regarded as significant or not. Fig. 1 presents more details of this selection process.

In Section 4, we present simulation results to demonstrate that the decryption scheme always recovers the encrypted ROI that results from the encryption scheme. This is due to the fact that the proposed encryption scheme possesses very good randomness properties, thus encrypted blocks have a high value for the parameter *e*. In this paper, we use the term sub-image to refer to the full image or its ROI, depending on whether we apply a full or selective encryption.

```
Read the input image into an $M \times N$ matrix $J$ of 24–bit integers (8 bits for each RGB band).
The parameters $\tau$ and $s$ represent the statistical threshold and the block size, respectively.
Partition $J$ into $p = MN/s^2$ blocks $B_1, B_2, \ldots, B_p$ of size $s \times s$.
For $k$ from 1 to $p$
    Let $c_{ij}$ denote the $(i,j)$–entry of $B_k$ and let $\bar{c}$ be the mean of the entries of $B_k$.
    Let $e = \sum_{i=1}^{s} \sum_{j=1}^{s} |c_{ij} - \bar{c}|$.
    If $e > \tau$
        Flag $B_k$ as part of the ROI.
    Else
        Flag $B_k$ as part of the ROB.
    End
End
```

Fig. 1. The selection of the ROI.