Commun Nonlinear Sci Numer Simulat 20 (2015) 447–460

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A symmetrical image encryption scheme in wavelet and time domain

Yuling Luo [a,*], Minghui Du [b], Junxiu Liu [a]

[a] Faculty of Electronic Engineering, Guangxi Normal University, Guilin 541004, China
[b] School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China

ARTICLE INFO

Article history:
Received 24 September 2012
Received in revised form 12 September 2013
Accepted 15 May 2014
Available online 3 June 2014

Keywords:
The spatiotemporal-chaos system
Image encryption
Integer wavelets transform (IWT)
Logistic map

ABSTRACT

There has been an increasing concern for effective storages and secure transactions of multimedia information over the Internet. Then a great variety of encryption schemes have been proposed to ensure the information security while transmitting, but most of current approaches are designed to diffuse the data only in spatial domain which result in reducing storage efficiency. A lightweight image encryption strategy based on chaos is proposed in this paper. The encryption process is designed in transform domain. The original image is decomposed into approximation and detail components using integer wavelet transform (IWT); then as the more important component of the image, the approximation coefficients are diffused by secret keys generated from a spatiotemporal chaotic system followed by inverse IWT to construct the diffused image; finally a plain permutation is performed for diffusion image by the Logistic mapping in order to reduce the correlation between adjacent pixels further. Experimental results and performance analysis demonstrate the proposed scheme is an efficient, secure and robust encryption mechanism and it realizes effective coding compression to satisfy desirable storage.

1. Introduction

With the rapid development of network and information technology, digital image has become an important access to acquire information, and a part of people's daily life. As a result, the security and storage of image data become an important requirement [1]. To improve the transfer efficiency and ensure the security of image data, encryption techniques were introduced in [2] and are becoming an increasing interest in both research and application fields. According to Shannon's confusion and diffusion principles of secure communication in [3], several theory-based encryption algorithms (such as Data Encryption Standard, International Data Encryption Algorithm and the algorithm developed by Rivest, Shamir and Adleman [4]) were firstly put forward. However, these traditional encryption schemes do not seem to be suitable for image data due to the intrinsic properties of image such as bulk data volume, high redundancy and local structure [5]. Therefore, other encryption schemes based on nonlinear functions are successively designed [6–33]. Among them, chaos can be viewed as a good candidate for image encryption scheme due to its analogous cryptography characteristics, such as extremely sensitive to initial conditions and system parameters, random-like and ergodicity [6].

The basic principle of chaos-based encryption schemes is to produce a long random sequence and encrypt a plain-image with the random sequence [7]. Fridrich applied chaos-based encryption method to image encryption for the first time in

* Corresponding author. Tel.: +86 (0)773 5857 296.
E-mail address: yuling0616@gxnu.edu.cn (Y. Luo).

http://dx.doi.org/10.1016/j.cnsns.2014.05.022
1007-5704/

1998 [8]. Chen et al. introduced a symmetric image encryption scheme based on 3D chaotic cat maps in 2003 [9]. Pareek et al. proposed two different encryption schemes based on one-dimensional and multiple one-dimensional chaotic maps, respectively in 2005 and 2006 [10,11]. An image encryption scheme was proposed in [12], which employed a novel image total shuffling matrix to shuffle the positions of image pixels and then used the states combination of two chaotic systems to confuse the relationship between the plain-image and the cipher-image. Different with these combined encryption schemes, a block encryption for image was proposed in [13] using combination of confusion and diffusion which did not confuse the original image directly, but generated a pseudo-random as a route for diffusion, and combined pixels to block randomly then arrayed them. Unfortunately, these encryption schemes have the weaknesses of small key space and low security because the chosen chaotic systems were either only one/two dimensional or simple 3D chaotic systems. To overcome these weaknesses, other image encryption schemes have been proposed which are based on a high-dimensional and complex chaotic system (including mixed chaotic systems [14], spatiotemporal chaos [15–18]) or performed in transform (such as Fourier transform, cosine transform [20], fractional Fourier transform (FrFT) [19,21], wavelet transform [22–25], fractional wavelet transform (FrWT) [26,27], etc.) domain. Compared to one/two dimensional or simple 3D chaotic maps, these new chaotic systems, especially the spatiotemporal chaos, greatly enhance the spatiotemporal complexity of nonlinear dynamics and mixture, which can effectively remedy the computer precision problem. On the other hand, transform domain schemes are more complex and are based on encrypting the transform coefficients of whole or some significant data to change all pixels of image through the inverse transform. In 2011, Zhu et al. proposed a novel image encryption scheme based on the improved hyper-chaotic sequences [14]. Sun and Lü proposed a secure approach for encryption and decryption of digital images with chaotic map lattices [15]. An CML-based spatiotemporal chaos system have been used in [16] for image blocks encryption, where the basic idea is to divide the image into blocks, and then use the block numbers as the spatial parameter of CML to iterate the chaos system to perform the substitution and diffusion for each block. Two approaches in [17,18] were proposed to realize the synchronization of the spatiotemporal chaos, which can achieved image encryption. In addition, Liu et al. proposed a triple image encryption scheme using of fractional Fourier transform in [19]. In this approach, the original image was encoded in amplitude part and other two images were encoded into phase information. And Liu et al. designed a color image encryption algorithm by using Arnold transform and color-blend operation in discrete cosine transform domains as well [20]. In 2011, a double image encryption method was proposed using fractional Fourier domain random encoding and pixel scrambling technique in [21]. And a chaos-based image encryption and compression algorithm was proposed in [22], which was realized by use of the properties of 2D wavelet transform. Meanwhile, two satellite image encryption schemes based on chaos and wavelet transform were proposed in [23] and [24], respectively. To decrease the computer cost, Amit et al. proposed a lightweight multimedia encryption strategy based on a modified discrete wavelet transform [25]. And Gaurav et al. proposed two chaos-based multimedia encryption schemes in fractional wavelet packet transform domain and fractional wavelet transform domain, respectively [26,27].

In this paper, a new image encryption technique is proposed based on nonlinear spatiotemporal chaotic map and integer wavelet transform (IWT). Compared with conventional permutation–diffusion process in transform domain, the proposed scheme is an opposite process. First, the original image is decomposed into the approximation and detail components using IWT, and only the approximation wavelet coefficients are encrypted and diffused with prime module congruence method (PMCM) and 2D spatiotemporal chaos operations. The approximation wavelet coefficients are deformed by random matrices generated from a spatiotemporal-chaos system, particularly the initial conditions of which are closely related to the plain-image to enhance the security. Then the inverse IWT is performed to get diffused image. To decrease the correlation among adjacent pixels of the diffused image further, the location of each pixel is shuffled by the Logistic map followed by obtaining the final encrypted image. For the decryption process, the encrypted image can be decrypted using the inverse operation. The experimental results and performance analysis demonstrate that the proposed encryption scheme can encrypt the image effectively and resist various typical attacks.

The rest of this paper is organized as followed. In Section 2, a spatiotemporal-chaos system and the PMCM algorithm are outlined. Section 3 presents the diffusion-permutation process for the proposed image encryption scheme. The experimental results and performance analysis are discussed in Section 4. Finally, Section 5 concludes this paper.

2. Preliminaries

This section introduces the basic background, including the theory of PMCM, IWT and spatiotemporal chaos which are employed to aid implementing the proposed encryption scheme.

2.1. Prime module congruence method (PMCM)

PMCM is a general pseudo-random number generator (PRNG). In [28], it is defined as Eq. (1) which is,

$$\begin{cases} x_n = a x_{n-1} \bmod M \\ r_n = x_n / M \end{cases} \tag{1}$$

where $M \in Z^+$ is the modulus and $a \in Z^+$ is the multiplication factor. $x_n \in [0, M]$ is the generated pseudo random sequence, and $r_n \in (0, 1)$ is the corresponding random decimal. In general, there are two specific types: $a = 3125$, $M = 2^{35} - 31$ and $a = 16807$, $M = 2^{31} - 1$.