Signal Processing: *Image Communication* 29 (2014) 618–627

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

An image encryption scheme based on irregularly decimated chaotic maps

M. Ghebleh [a], A. Kanso [a,*], H. Noura [b]

[a] *Department of Mathematics, Kuwait University, P.O. Box 5969, Safat 13060, Kuwait*
[b] *Universite Paris SUD, Laboratoire de Recherche en Informatique, Orsay, France*

ARTICLE INFO

Article history:
Received 8 July 2013
Received in revised form
8 September 2013
Accepted 10 September 2013
Available online 4 October 2013

Keywords:
Chaos
Cryptography
Image encryption
Arnold cat map
Skew tent map

ABSTRACT

An image encryption scheme provides means for securely transmitting images over public channels. In this work, we propose a robust shuffling–masking image encryption scheme based on chaotic maps. The shuffling phase permutes square blocks of bytes using a 3-dimensional chaotic cat map coupled with a zigzag scanning procedure. The masking phase then scrambles b-byte blocks of the shuffled image with combined outputs of three 1-dimensional chaotic skew tent maps, in such a way that the masking of every block is influenced by all previously masked blocks. Empirical results show that while the suggested scheme has good running speed, it generates ciphered images that exhibit (i) random-like behavior, (ii) almost flat histograms, (iii) almost no adjacent pixel correlation, (iv) information entropy close to the ideal theoretical value. Furthermore, this scheme has a large key space, strong sensitivity to the secret key, and is robust against differential attacks. On the basis of these results, this scheme can be regarded as secure and reliable scheme for use in secure communication applications.

1. Introduction

With the rapid advancement of communication technology, nowadays more and more text, image, audio, video and other multimedia files are transmitted over the internet. However, any type of data transmitted over a public channel such as the internet can be intercepted by an eavesdropper and hence become subject to security threats. Thus, means of secure transmission of data has become a necessity. One of the most important security issues is data confidentiality which can be addressed using a practical and secure encryption scheme. Most traditional encryption schemes that have appeared in the literature such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest, Shamir and Adleman (RSA), ElGamal schemes [1,2] and other chaotic encryption schemes [3–8] mainly protect textual data. Image encryption schemes differ from text encryption schemes as digital images are characterized by the existence of bulk data capacity and high redundancy. Some of the aforementioned encryption schemes are not ideal for encryption of digital images as they suffer from low speed. On the other hand, many chaos-based image encryption schemes have been suggested in the literature [9–26]. Some of these schemes have been shown to have security flaws [27–42]. Therefore, designing fast and efficient image encryption schemes remains a major challenge for researchers.

In [9,11,20,25], a general shuffling–making structure for chaotic image encryption schemes was suggested. The shuffling phase permutes the pixels of a digital image without modifying their values, while the masking phase scrambles the shuffled pixels in a way that any modification of a pixel affects as many pixels as possible. In this paper, we propose a chaotic image encryption scheme within this shuffling-masking paradigm. The proposed scheme takes as input a digital image of any size, say

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

0923-5965/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.image.2013.09.009

$m \times n \times 3$, where the third dimension accounts for the RGB channels, and produces a random noise-looking ciphered image. The shuffling phase divides the input image into square blocks of fixed side length ℓ, and shuffles them according to an orbit of a 3-dimensional (3D) chaotic cat map. The resulting block-shuffled image is then rearranged via a zigzag scanning procedure to generate a 1-dimensional (1D) array of bytes. The masking phase scrambles the resulting sequence in b-byte blocks, where b is an even number fixed as a parameter of the masking algorithm. Each b-byte block is masked with a b-byte block R of pseudo-random integers in $[0, 255]$ in such a way that the masking of each block is influenced by all previously masked blocks. The pseudo-random block R is generated by combining outputs of three 1D chaotic skew tent maps iterated according to an irregular decimation rule. The use of irregularly decimated orbits increases the security of the proposed encryption algorithm. This is due to the existence of methods, such as those presented in [43,44], which can be used to estimate the initial conditions and parameters of a chaotic map from its orbits. The suggested scheme overcomes some security flaws in the existing image encryption algorithms [9,24] and provides a high level of confusion and diffusion. Furthermore, it has a large key space, and it defeats some well-known cryptanalytic attacks such as differential attacks and those presented in [41,42].

This paper is organized as follows. Section 2 presents the proposed scheme. This section contains brief introductions to the chaotic maps used in the shuffling and masking phases of the proposed algorithm. In Section 3, the performance of the proposed algorithm is analyzed by means of various statistical and security tests. Finally, some concluding remarks are presented in Section 4.

2. The proposed image encryption scheme

In this section, we provide a detailed description of the proposed chaos-based image encryption scheme. This scheme consists of two phases: the shuffling phase and the masking phase. The shuffling phase employs a 3D chaotic cat map to permute square blocks of the plain image, whereas the masking phase uses mixed orbits of chaotic skew tent maps to mask b-byte blocks of the shuffled image. In the following subsection, we describe the chaotic maps which are used as building blocks in the design of the proposed scheme.

2.1. The chaotic maps

Since the early 1990s, chaotic maps have been used in the design of many algorithms including encryption, hashing, watermarking and steganography. In this study, two of the most frequently used chaotic maps, the cat map and the skew tent map are employed. The Arnold cat map is a 2D map defined by [47] and used for image encryption in [9,10]. It is given by

$$F(X_i) = X_{i+1} = \begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} (\text{mod } 1), \tag{1}$$

where the state $(x_i, y_i) \in [0,1) \times [0,1)$, for $i = 0, 1, \ldots$, and (x_0, y_0) is referred to as its initial condition. This map possesses chaotic behavior and is area preserving [9]. Chen et al. [9] propose a generalization of Eq. (1) into a 2D cat map by introducing two parameters. Furthermore, they extend this generalization to a 3D variant of the cat map. This 3D variant of the cat map is defined by

$$F(X_i) = X_{i+1} = \begin{bmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} (\text{mod } 1), \tag{2}$$

where

$$\mathbf{A} = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y b_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}, \tag{3}$$

and $a_x, a_y, a_z, b_x, b_y, b_z$ are positive integers. It is easy to see that A has determinant 1.

In the shuffling phase of the proposed scheme, we use a 3D variant of the cat map defined in Eq. (2) with $a_x = a_y = a_z = 2$ and $b_x = b_y = b_z = 1$. That is,

$$F(X_i) = X_{i+1} = \begin{bmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{bmatrix} = \begin{bmatrix} 5 & 2 & 14 \\ 7 & 3 & 20 \\ 3 & 1 & 9 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} (\text{mod } 1). \tag{4}$$

The above map is area preserving since the transformation matrix A has determinant 1. On the other hand, A has eigenvalues $\lambda_1 = 0.1019, \lambda_2 = 0.5606$, and $\lambda_3 = 16.3301 > 1$. Thus, the map of Eq. (4) exhibits chaotic behavior such as high sensitive dependence on initial conditions and control parameters, unpredictability of the generated orbits, random-like behavior, etc.

In the masking phase of the proposed scheme, we employ the skew tent map, also known as the asymmetric tent map, which is a 1D chaotic map. The skew tent map is widely used in cryptographic applications [48,49] and is given by

$$G_p(x_i) = x_{i+1} = \begin{cases} \dfrac{x_i}{p} & \text{if } 0 \le x_i \le p \\ \dfrac{1 - x_i}{1 - p} & \text{if } p < x_i \le 1, \end{cases} \tag{5}$$

where $x_i \in [0,1]$ and $p \in (0,1)$ are the state and control parameter of the map, respectively. For $p \in (0,1)$, the map defined in Eq. (5) has a positive Lyapunov exponent and therefore, it demonstrates chaotic behavior [48]. Furthermore, as shown in [48,49], the orbits $\{x_i\}_{i=0}^{\infty}$ of this map are uniformly distributed over the interval $[0,1]$.