Commun Nonlinear Sci Numer Simulat 20 (2015) 846–860

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism

Jun-xin Chen [a], Zhi-liang Zhu [b,*], Chong Fu [a], Hai Yu [b], Li-bo Zhang [b]

[a] School of Information Science and Engineering, Northeastern University, No. 11, Lane 3, WenHua Road, Shenyang 110004, Liaoning, China
[b] Software College, Northeastern University, No. 11, Lane 3, WenHua Road, Shenyang 110004, Liaoning, China

ARTICLE INFO

Article history:
Received 2 November 2013
Received in revised form 12 June 2014
Accepted 18 June 2014
Available online 3 July 2014

Keywords:
Image encryption
Dynamic state variables selection
Pixel-swapping based confusion
Snake-like diffusion

ABSTRACT

In recent years, a variety of chaos-based image cryptosystems have been investigated to meet the increasing demand for real-time secure image transmission. Most of them are based on permutation–diffusion architecture, in which permutation and diffusion are two independent procedures with fixed control parameters. This property results in two flaws. (1) At least two chaotic state variables are required for encrypting one plain pixel, in permutation and diffusion stages respectively. Chaotic state variables produced with high computation complexity are not sufficiently used. (2) The key stream solely depends on the secret key, and hence the cryptosystem is vulnerable against known/chosen-plaintext attacks. In this paper, a fast chaos-based image encryption scheme with a dynamic state variables selection mechanism is proposed to enhance the security and promote the efficiency of chaos-based image cryptosystems. Experimental simulations and extensive cryptanalysis have been carried out and the results prove the superior security and high efficiency of the scheme.

1. Introduction

With the dramatic development of communication technologies, digital image application and exchange across Internet have become much more prevalent than the past. Cryptographic approaches are therefore critical for secure image transmission and storage over public networks. However, traditional encryption algorithms are typically designed for textual information and have been found not suitable for image encryption due to some intrinsic features of images such as high pixel correlation and redundancy [1]. Since 1990s, many researchers have noticed that the fundamental features of chaotic systems such as ergodicity, mixing property, unpredictability, sensitivity to initial conditions/system parameters, *etc.* can be considered analogous to some ideal cryptographic properties for image encryption [2,3]. In 1998, permutation–diffusion architecture for chaos-based image encryption was firstly proposed by Fridrich [4]. Under this structure, a plain image is firstly shuffled by a two-dimensional area-preserving chaotic map with the purpose to erase the high correlation between adjacent pixels. Then pixel values are modified sequentially using pseudorandom key stream elements produced by a certain qualified chaotic map in the diffusion procedure. This architecture forms the basis of numerous chaos-based image cryptosystems proposed subsequently [5–28]. During the past decades, improvements to this architecture have been extensively developed in various aspects, such as novel pixel-level confusion techniques [5–9], bit-level permutation approaches

* Corresponding author. Tel.: +86 24 86581232.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.cnsns.2014.06.032
1007-5704/

[10–14], improved diffusion strategies [15–19], applications of plain-image related parameters [20–22] and enhanced key stream generators [23–28].

Meanwhile, recent cryptanalysis works have demonstrated that some chaos-based image cryptosystems are insecure against various attacks, and have been successfully broken [29–36]. The weaknesses in these insecure algorithms include insensitiveness to the changes of the plain image, weak secret keys, and the most serious one is that the key stream is completely depending on the secret key. That means identical key stream will be used to encrypt different plain images if the secret key remains unchanged. This property allows the attacker to launch known-plaintext attack [30–33,35] or chosen-plaintext attack [30,31,33,35,36] so as to retrieve the equivalent key stream elements. Therefore, to further enhance the security, the key stream elements extracted from the same secret key should better be distinct and related to the plain image [20]. Some general rules for evaluating the security performance of a chose-based cryptosystem can be found in [1,2]. Besides, the permutation and diffusion are treated as two independent procedures in most of the existing image cryptosystems. Two-dimensional and one-dimensional chaotic maps are generally employed to achieve cryptographic requirements in the permutation and diffusion stages, respectively. Chaotic state variables generated in both stages are merely used for respective encrypting operation, which means at least two chaotic state variables are required for ciphering one pixel. Chaotic state variables that are calculated with high computation complexity are not sufficiently used. The present paper proposes a novel chaos-based image encryption scheme with a dynamic state variables selection mechanism (DSVSM). This cryptosystem can satisfy the security requirements suggested in [1,2] and well address the flaws existing in the cracked algorithms by employing innovations in four aspects. (1) Chaotic state variables used in our cryptosystem are generated from three-dimensional or hyper chaotic systems, and will be shared in permutation and diffusion procedures. Accordingly, a slight change in the secret key will not only affect the diffusion module but also influence the permutation procedure simultaneously. Besides, the chaotic state variables sharing mechanism can also significant advance the utilization efficiency of the chaotic map iteration. (2) The state variable allotted for each pixel's encryption is decided by DSVSM, which is plain pixel-related. When ciphering different plain images, distinct key streams will be produced both in the permutation and diffusion procedures, even though adopt the same secret key. The attacker cannot obtain useful information by encrypting some special images, as the resultant information is self-related to the chosen-images. This property ensures the resistance to known/chosen-plaintext attacks. (3) Pixel-swapping based image confusion approach is proposed as a replacement of the traditional permutation approaches. This confusion strategy can produce confusion and certain diffusion effects simultaneously in the permutation stage, so as to accelerate the overall diffusion effect of the cryptosystem. (4) Image diffusion in our scheme is implemented in snake-like mode. In coordination with the pixel-swapping based confusion strategy and DSVSM, the difference spreading effect produced in the confusion stage can be further scattered to the whole cipher image in the first round diffusion. The efficiency of the cryptosystem is therefore remarkably improved. Experiment results demonstrate that the proposed scheme has a high security level and satisfactory operation efficiency for practical secure image applications.

The remaining of this paper is organized as follows. In next section, the architecture of typical chaos-based image cryptosystems is introduced. Then the proposed image encryption scheme will be described in detail in Section 3. Simulation results, the effectiveness and efficiency of the proposed scheme are reported in Section 4. Thorough security analyzes of the cryptosystem are carried out in Section 5. Finally, conclusions will be drawn in the last section.

2. Architecture of typical chaos-based image cryptosystems

The architecture of typical chaos-based image cryptosystems is shown in Fig. 1. There are two stages in the cryptosystems of this kind, namely, the permutation stage and diffusion stage.

In the permutation stage, image pixels are generally shuffled by a two-dimensional area-preserving chaotic map, without any modification to their values. Traditionally, three types of chaotic maps, Arnold cat map, standard map and baker map are employed, and their discretized versions are given by Eqs. (1)–(3), respectively.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \bmod N, \tag{1}$$

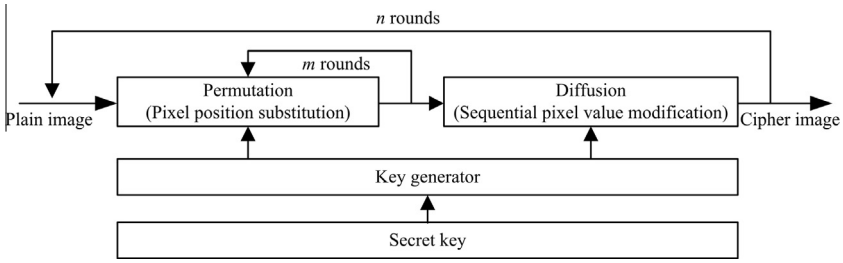

Fig. 1. The architecture of typical chaos-based image cryptosystems.