Optik 125 (2014) 2472–2478

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme

Jun-xin Chen [a,*], Zhi-liang Zhu [b], Hai Yu [b]

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China

ARTICLE INFO

Article history:
Received 25 May 2013
Accepted 24 October 2013

Keywords:
Image encryption
Chaos
Arnold cat map
Continuous diffusion

ABSTRACT

In recent years, a number of chaos-based image cryptosystems have been proposed to meet the increasing demand for real-time secure image transmission. In this paper, an improved diffusion scheme named continuous diffusion strategy is proposed to promote the efficiency of the conventional permutation–diffusion type image cipher. The new scheme contains a supplementary diffusion procedure after the conventional diffusion process and the control parameters are altered by the cipher image after the first diffusion procedure. As a result, the difference can be introduced at the beginning and spread out to the whole image, and hence the same level of security can be achieved with fewer overall rounds. Moreover, to further enhance the confusion effect of the diffusion operation, an intensive diffusion approach is proposed, using stretched key stream elements to perform a cyclic shift to the cipher pixels. Extensive cryptanalysis has been performed using differential analysis, key space analysis, key sensitivity analysis and various statistical analyses. Experiment results demonstrate that the new scheme has a high level of security and fast encryption speed for practical image encryption.

1. Introduction

With the dramatic development of communication technology, multimedia content, which takes digital image as its core, has become the crucial element in the prospective information transmission. Consequently, cryptographic approaches for digital image are critical for secure image transmission over public networks. However, conventional data encryption algorithms such as Triple-DES, IDEA, AES and other symmetric cryptographic algorithms are found poorly suited for digital images characterized with some intrinsic features such as high pixel correlation and redundancy [1]. In this regard, chaos-based image cipher has been widely investigated since the late 1990s, as many researchers have noticed that there exists a natural relationship between chaos and cryptography.

In [2], Fridrich suggested that a chaos-based image encryption scheme should compose of two stages: permutation and diffusion. In the first stage, pixels are shuffled by a two-dimensional chaotic map, then pixel values are modified sequentially using a certain discretized or continuous chaotic map in the second stage. Based on this architecture, a number of chaos-based image ciphers are proposed subsequently [1,3–21]. In [3,4], Chen and his group employed a 3D chaotic cat map and baker map in the permutation stage, respectively. In [5], Lian et al. suggested using a standard map in permutation process and a quantized logistic map in the diffusion stage. The parameters of these two chaotic maps are determined by a key stream generated in each round. In [6], Wang et al. proposed a chaos-based image encryption algorithm with variable control parameters with the purpose of resisting known/chosen plaintext attacks. In [7,8], two kinds of bit-level shuffling algorithms are proposed, which can introduce a significant diffusion effect in permutation stage. In order to achieve larger key space and overcome the weak security in one-dimensional chaotic system, hyperchaotic systems were employed for image encryption in [9–11], multi chaotic systems or coupled nonlinear chaotic map were used in [12–16], while in [17,18], spatial chaos maps are employed.

Besides the algorithms listed above, whose achievements focus on security improvements, there are few ciphers deal with efficiency issues. In [1], a lightweight table lookup and swapping technique was proposed to address the efficiency problem encountered by substitution-diffusion type chaos-based image cryptosystems. In [19], a cryptosystem that can introduce certain diffusion effect in the permutation stage is proposed to reduce the workload of the time-consuming diffusion procedure. As a result, fewer over all rounds and hence a shorter encryption time is obtained. In [20], Xiang et al. proposed a selective gray-level image encryption scheme, in which only 50% of the whole image data is encrypted, and therefore the encryption time is reduced. In [21], Fu

* Corresponding author.
E-mail address: junxin_chen@qq.com (J.-x. Chen).

0030-4026/$ – see front matter © 2014 Published by Elsevier GmbH.
http://dx.doi.org/10.1016/j.ijleo.2013.12.001

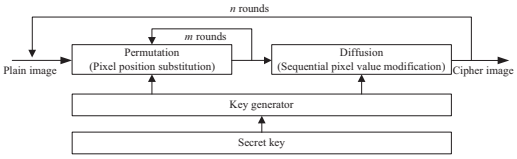

Fig. 1. Typical architecture of the chaos-based image cryptosystems.

et al. proposed an improved diffusion strategy named bidirectional diffusion. By using this strategy, the spreading process can be significantly accelerated and hence the same level of security can be achieved with fewer overall encryption rounds.

As pointed out by many previous works, the diffusion process is the highest cost of the whole cryptosystem. This is because a considerable amount of computation load is devoted to chaotic map iteration and quantization operation that is required by the key stream generation. Therefore, the critical issue of a fast image cipher is how to reduce the diffusion rounds, while keeping its security level. In this paper, we propose a continuous diffusion scheme which consists of two relevant diffusion rounds in one overall round encryption, while in the supplementary diffusion procedure, control parameters are altered by the cipher image generated after first diffusion stage. As a result, the difference can be introduced at the beginning and spread out to the whole cipher image throughout the supplementary diffusion process. To further enhance the security, an intensive diffusion approach is employed. By performing cyclic shift operation to the cipher pixels, which is controlled by the stretched chaotic key stream elements, the influence of the chaotic map can be injected to the cipher image on the other hand. Experimental results show that the new scheme can accelerate the spreading process remarkably and a satisfactory security level can be obtained with only one overall cipher cycle. The remainder of this paper is organized as follows. Section 2 presents the architecture of the chaos-based image cipher. Then the proposed diffusion scheme is described in more detail in Section 3. Simulation results, the effectiveness and efficiency of the proposed scheme are reported in Section 4. Detailed security analyses of the cryptosystem are carried out in Section 5. Finally, conclusions are drawn in the last section.

2. Architecture of the chaos-based image cryptosystems

A typical architecture of the chaos-based image cryptosystems is shown in Fig. 1.

As shown above, there are two stages in the typical chaos-based image cryptosystem, permutation and diffusion. In this paper, Arnold cat map [22], a kind of two-dimensional area-persevering chaotic map, is employed in the permutation stage to shuffle the positions of the plain image pixels and weaken the relationship between adjacent pixels. The mathematical formula of Arnold cat map is given by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1, \quad (1)$$

where "x mod 1" represents the fractional parts of a real number x. The 2D cat map can be generalized by introduced two parameters to Eq. (1), as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1. \quad (2)$$

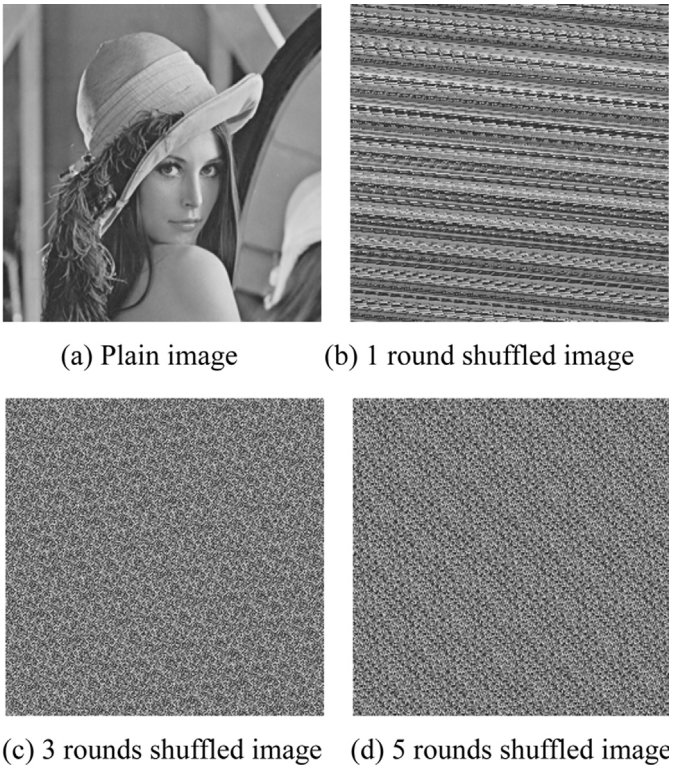

Fig. 2. The application of cat map with different rounds.

In order to employ the generalized 2D Cat map in image encryption, it has to be discretized first, as described by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N. \quad (3)$$

Essentially, the discretization process is to impose restrictions on value limit of cat map, only positive integer is allowed, while reserving the features such as mixing property and the sensitivity to initial parameters. Parameters p, q and the number or iterations m can be used as secret keys.

The inverse transform used for decryption is expressed in Eq. (4).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N. \quad (4)$$

The application of the cat map to a grayscale test image with 256×256 size is demonstrated in Fig. 2, the permutation key is "$p = 5$, $q = 10$". Fig. 2(a) shows the plain image, Fig. 2(b)–(d) shows the results of applying the discretized cat map once, three and five times, respectively.

As can be seen from Fig. 2, after three rounds iteration, the correlation among adjacent pixels is wholly disturbed and the image is completely unrecognizable. However, without changing the pixel value, the statistical property of the shuffled image is unchanged. Therefore, the shuffled image is weak against statistical attack and known plain-text attack. As a remedy, a diffusion procedure is employed next to improve the security.

In diffusion stage, the pixel values are modified sequentially by mixing the plain-pixel with the key stream elements which are generated by chaotic map so as to confuse the relationship between cipher image and plain image. The cipher-pixel value is obtained according to

$$c(n) = k(n) \oplus \{[p(n) + k(n)] \bmod N\} \oplus c(n-1), \quad (5)$$