Commun Nonlinear Sci Numer Simulat 19 (2014) 3653–3659

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A chaotic image encryption scheme owning temp-value feedback

Leo Yu Zhang [a,*], Xiaobo Hu [b], Yuansheng Liu [c], Kwok-Wo Wong [a], Jie Gan [b]

[a] Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China
[b] State Grid Electric Power Research Institute, Beijing 100192, China
[c] College of Information Engineering, Xiangtan University, Xiangtan 411105, Hunan, China

ARTICLE INFO

Article history:
Received 15 April 2013
Accepted 17 March 2014
Available online 24 March 2014

Keywords:
Image encryption
Chen system
Logistic map
Permutation
Diffusion

ABSTRACT

Many round-based chaotic image encryption algorithms employ the permutation–diffusion structure. This structure has been found insecure when the iteration round is equal to one and the secret permutation of some existing schemes can be recovered even a higher round is adopted. In this paper, we present a single round permutation–diffusion chaotic cipher for gray image, in which some temp-value feedback mechanisms are introduced to resist the known attacks. Specifically, we firstly embed the plaintext feedback technique in the permutation process to develop different permutation sequences for different plain-images and then employ plaintext/ciphertext feedback for diffusion to generate equivalent secret key dynamically. Experimental results show that the new scheme owns large key space and can resist the differential attack. It is also efficient.

1. Introduction

In the information era, digital images have been widely used for various applications, such as entertainment, business, health service and military affairs. All the sensitive data should be encrypted before transmission to avoid eavesdropping. However, bulk data size and high redundancy among the raw pixels of a digital image make the traditional encryption algorithms, such as DES, IDEA, AES, not able to be operated efficiently. Therefore, designing specialized encryption algorithms for digital images has attracted much research effort. Some intrinsic properties of chaotic systems, such as ergodicity, sensitive to the initial condition and control parameters, are analogous to the confusion and diffusion properties specified by Shannon [1]. Thus makes it natural to employ chaotic systems in image encryption algorithms [2–10]. Meanwhile, the art of cryptanalysis has also made new achievements in the last few decades. Some of the existing image encryption algorithms are found insecure [11–18] to different degrees due to the following defects: (1) the (equivalent) secret key can be obtained by the brute-force attack due to the dynamical degradation of chaotic systems in digital domain; (2) all the operations employed in the encryption process are reversible without the key or even linear, therefore the mathematical model of the scheme is not a keyed one-way function [19]. In [20], some basic requirements for evaluating the chaotic encryption algorithms are concluded.

The permutation–diffusion structure becomes the basis of many chaotic image encryption schemes since Fridrich developed a chaos-based image encryption scheme of this structure in 1998 [2]. The symmetric image encryption scheme in [4]

* Corresponding author at: Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China. Tel.: +852 6064 6806.
E-mail address: leoxtu@gmail.com (L.Y. Zhang).

http://dx.doi.org/10.1016/j.cnsns.2014.03.016
1007-5704/

extended the Cat map to three-dimensional to make it suitable for permutation in space, followed by a similar diffusion construction of Fridrich's. In 2004, Mao et al. proposed an image encryption algorithm, where the discrete Baker map was employed for permutation [8]. It's worth mentioning that most image encryption schemes of this structure have to execute the permutation and diffusion procedures alternatively for several rounds to fulfill the security requirement, which will certainly lead to some reduction in efficiency. Nonetheless, Solak et al. proposed a chosen ciphertext attack in 2010 by utilizing the relationship between the pixels in the neighboring encryption rounds [12]. This attack is efficient for Fridrich's scheme [2] and it can also be applied to Chen's scheme [4]. In addition, it is reported in [21] that the equivalent key of several permutation–diffusion image ciphers, such as those suggested in [2,4,8,22], can be recovered when only one encryption round is applied.

Meanwhile, image encryption algorithms having other structures have also been developed. In 2010, Patidar et al. suggested a substitution–diffusion structure for color image [10], which was attacked in [18]. In [9], Huang et al. presented a multi-chaotic system based permutation scheme, in which pixel positions and bits in the individual pixel are shuffled together to achieve permutation and substitution simultaneously. Intuitively, permutation-only schemes are not secure against known/chosen plaintext attack. In [13,17], Li et al. proposed the quantitative and optimal quantitative cryptanalysis of the permutation-only encryption schemes with respect to known/chosen plaintext attack.

By combining the Chen system and the Logistic map, a novel permutation–diffusion image encryption algorithm is proposed in this paper. To resist the known attacks and achieve better efficiency, two temp-value feedback mechanisms are embedded into a single permutation–diffusion round. In the permutation part, we develop different permutation sequences for different plain-images by means of mapping some information of the plain-image to the generation process of the permutation sequence. Thus makes the permutation behave in a "one time pad" manner. In the diffusion part, another feedback technique is employed to make the equivalent key generation depend on both the plain-image and the temp-value. By combining the proposed permutation and diffusion technique, the scheme frustrates the known attacks [12,21]. In addition, we add a reversely-executed diffusion process to make the scheme sensitive to changes of plain-image.

The rest of this paper is organized as follows. Section 2 presents some descriptions of the prerequisites of the algorithm, such as expanded XOR operation, the temp-value feedback mechanism, followed by the detailed encryption/decryption procedures. In Section 3, we evaluate the new scheme via numerical simulations and comparisons. The last section gives some concluding remarks.

2. The proposed image encryption algorithm

2.1. The involved chaotic systems

Chen system has been widely adopted in many chaotic image encryption algorithms, it can be modeled by [4]

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where a, b and c are system parameters. The system is chaotic when $a = 35$, $b = 3$ and $c \in [20, 28.4]$. In the proposed encryption algorithm, c is fixed at 28.

The other chaotic system employed in this encryption algorithm is the Logistic map

$$y_{n+1} = \mu \cdot y_n \cdot (1 - y_n),$$

where $y_n \in (0, 1)$ and μ is the control parameter. When $\mu \in (3.5699456, 4)$, the output sequence is ergodic in the unit interval $(0,1)$, which makes the Logistic map suitable for pseudorandom number generation [23].

2.2. The expanded XOR operation

The expanded XOR (eXOR) operation is introduced to enhance the overall security level of the scheme. For two inputs $x = \sum_{i=0}^{7} x_i$ and $r = \sum_{i=0}^{8} r_i$,

$$\mathrm{eXOR}(x, r) = \sum_{i=0}^{7} \mathrm{not}(x_i \oplus r_i \oplus r_{i+1}) \cdot 2^i,$$

where $\mathrm{not}(x)$ flips a single bit x. Then one can deduce a property of eXOR as follows.

Property 1. *If the equation*

$$\mathrm{eXOR}(x, r) = t$$

holds, then

$$\mathrm{eXOR}(t, r) = x.$$