Neurocomputing 283 (2018) 53–63

Contents lists available at ScienceDirect

Neurocomputing

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

Designing permutation–substitution image encryption networks with Henon map

Ping Ping*, Feng Xu, Yingchi Mao, Zhijian Wang

College of Computer and Information, Hohai University, Nanjing 210098, China

ARTICLE INFO

Article history:
Received 8 July 2017
Revised 11 October 2017
Accepted 15 December 2017
Available online 27 December 2017

Communicated by Liu Guangcan

Keywords:
Image encryption
Cryptosystem
Chaotic cryptography
Henon map

ABSTRACT

In traditional permutation–substitution architecture type image cipher, the permutation and substitution generally are two independent parts, and the diffusion performed by substitution is more like the cipher block chaining mode of operation. However, such operation approaches clearly downgrade the encryption efficiency because the pixel values need to be modified one by one for 2–4 overall rounds and images are scanned twice for permutation and substitution in each round. To improve the encryption efficiency, a new two-point diffusion strategy realized by discrete Henon map is proposed in this paper, which can significantly accelerate the diffusion process if there is more than one processing unit. Besides, the permutation and substitution are no longer two independent parts and they intermingle with each other so that the image required to be scanned just one time. To achieve the better ability of resisting chosen-plaintext or known-plaintext attack, the substitution keystream generated in our method is dependent on the plain image. Consequently, different plain images produce the distinct keystream for substitution. The results of various security analyses prove that our proposed image cryptosystem owns superior security, meanwhile, time complexity analysis shows that it can achieve faster encryption speed than most typical image encryption schemes.

1. Introduction

Nowadays, image security is becoming increasingly important as more and more confidential images are transmitted over public Internet or stored in a third party. In this respect, various image cryptosystems have been suggested because encryption is recognized as an effective and direct technique to keep private information safe. According to architectures, the methods for image encryption could be divided into three distinct categories: permutation-only, substitution-only and permutation–substitution. Generally, the permutation-only image encryption is commonly referred to as a lightweight image cipher. In [17,40], a pure image permutation algorithm was realized by bit-level permutation and a single chaos map. In [9], the authors presented a two-stage bit-level image permutation algorithm in order to introduce diffusion effect in permutation stage. However, the permutation-only encryption schemes are vulnerable to some powerful attacks [18,20,45]. For the substitution-only image cipher, Zhu [46] introduced a novel hyperchaotic sequences based image cipher with only two rounds diffusion operation. But, Özkaynak et al. [25] demonstrated that the secret parameters of this image cipher could be broken with chosen-plaintext attack, and Li et al. [19] re-evaluated the security of Zhu [46] and found it was very weak against known-plaintext attack. In [42], the authors put forward a new chaos based image cipher which only employs substitution function. Although it claimed that the scheme could withstand the chosen/known-plaintext attacks by error introducing, Yap and Phan [39] presented both chosen-ciphertext attack and chosen-plaintext attack against this scheme.

Compared with former two structures, the permutation–substitution (also known as confusion–diffusion) which was first proposed by Fridrich [7] is the most widely used architecture for image encryption [13,16,32,37,38,41]. Under this structure, the pixel positions are firstly shuffled in the permutation process for the sake of decreasing the strong correlation between pixels adjacent to each other. After that, values of the pixels are changed one by one in the substitution process to achieve the avalanche effect. All the stages of permutation and substitution repeat for multiple times with the purpose of obtaining a good security level. For example, a novel ideal of using two chaotic maps and the permutation–substitution structure for image encryption was suggested by Chen et al. [3]. In this approach, 3D chaotic cat map was utilized during the permutation stage to change the pixel positions while Logistic map was used in substitution process. The parameters of the above two maps were

* Corresponding author.
E-mail address: pingpingnjust@163.com (P. Ping).

https://doi.org/10.1016/j.neucom.2017.12.048
0925-2312/© 2018 Elsevier B.V. All rights reserved.

generated from the Chen's chaotic system. In [34], Wang et al. improved the permutation–substitution structure by introducing variable control parameters which makes known/chosen-plaintext attacks infeasible. In [43], Ye et al. introduced a two-way diffusion method for the purposed of improving the diffusion effect. In [8], Fu et al. put forward an optimized bidirectional-diffusion strategy which can promote the efficiency of the image cipher by reducing the overall encryption rounds. In [4], considerable diffusion effect was introduced before the diffusion procedure for a lower load to the time-consuming diffusion part. In [5], a new method of preserving and reusing the permutation matrix in the diffusion part was presented so as to improve the operation efficiency.

As can be seen from the above discussion, a number of improvements in security or efficiency have been made to traditional permutation–substitution type image ciphers. However, some efficiency weaknesses and insecurities can be found from many proposed image ciphers. First, the diffusion is the most time-consuming stage of the whole cryptosystem for most image cryptosystems. This is because the pixel values need to be modified one by one for 2–4 overall rounds so that each pixel depends on all previous processed pixels. Such diffusion strategy cannot be parallelized and is not suitable for real-time application. Second, most permutation-substitution type image ciphers treat permutation and substitution as two stages. As a result, an image pixel needs to be processed twice in each round, one for permutation and another for diffusion. Third, some permutation-substitution type image ciphers are vulnerable to chosen-plaintext or known-plaintext attack [1,29,30]. For example, Wang et al. [33] proposed a successful chosen-plaintext cryptanalytic attack on a 3D Cat map based symmetric image cipher [3]. Bechikh et al. [2] pointed out that the method proposed by Song et al. [31] was weak against chosen-plaintext attack because the substitution keystream is the same for every plainimage/cipherimage pair.

To further enhance the efficiency and security of the image cipher, we propose an efficient permutation - substitution image encryption network with Henon map. In order to improve the encryption efficiency, we present a new two-point diffusion strategy which is able to process two pixels simultaneously. Hence, the diffusion process would be significantly accelerated if there is more than one processing unit. Besides, the permutation and diffusion are no longer two independent parts in our improved architecture. As soon as a new pixel position is calculated, the pixel value is modified instead of calculating the next pixel position. The permutation and diffusion stages are merged so that the image pixel matrix required to be scanned just one time in each round. Thus, the improved permutation - substitution architecture is more efficient. For the sake of achieving the better ability of resisting chosen-plaintext or known-plaintext attack, the substitution keystream generated in our method is dependent on the plain image. As a result, different plain images produce the distinct keystream for substitution. It is difficult for an attacker to obtain any useful information about the keystream by a number of possible plainimage/cipherimage pairs. Two image features are inserted into the cipher image instead of transmitting them, which makes the image cipher still a symmetric cipher. Computer experiments and performance analyses prove that the our image encryption scheme not only owns superior security but also has low time complexity.

The rest of this paper is organized as follows. In Section 2, the basic theory about two-dimensional Henon map is introduced and the architecture of the proposed scheme is presented. Section 3 describes the proposed images encryption algorithm. Section 4 shows our computer simulations and results. Security and performance analyses are given in Section 5 and our conclusions are left to the final Section.

Fig. 1. Plain image with 256 gray levels.

2. Preliminaries

2.1. Two-dimensional Henon map

Chaotic systems have many unique proeprties such as ergodicity, unpredicabilty and initial state sensitivety [11,12,23]. These properties are very similar with the concept of image encryption [24]. Thus, chaotic systems are popular to design image encryption schemes. Here, we introduce the two-dimensional Henon map, and use it to develop our image encryption scheme. The Henon map defined on a two-dimensional plane is a nonlinear discrete-time dynamical system. It has been introduced and studied for the first time by Henon [10] in 1976. The Henon map is a 2-dimensional iterated map defined by

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

Here, x, y are iterated values while $n = 0, 1, 2, \ldots$ represents the number of map iterations. a, b are two control parameters that the map depends on. In the case of the Henon map with parameters $a = 1.4$ and $b = 0.3$, this dynamical system can display chaotic behaviors. For the classical Henon map defined by Eq. (1), it can be seen that the iterated time is discrete but the iterated values are continuous. In order to avoid the time-consuming operations such as converting floating-point number into binary number or sorting floating-point number in image cryptosystems, the Henon map is discretized and implemented in the integer domain [27]. After discretization, the Henon map becomes

$$\begin{cases} x_{n+1} = (1 - ax_n^2 + y_n) \bmod N; \\ y_{n+1} = (x_n + d) \bmod N, \end{cases} \tag{2}$$

where $x, y \in \{0, 1, 2, \ldots, N-1\}$ are discrete iterated values, $a, d \in \{1, 2, \ldots, 2^{128}\}$ denote two control parameters of discrete Henon map, N indicates the order of digital image matrix. Obviously, the discrete Henon map is reversible. The inverse transformation is defined as

$$\begin{cases} x_n = (y_{n+1} - d) \bmod N; \\ y_n = (x_{n+1} - 1 + ax_n^2) \bmod N. \end{cases} \tag{3}$$

Since the discrete Henon map is a one-to-one map and there only exists integer calculations, it may be quite simple and efficient to permute image pixels with the iteration of the discrete Henon map. In the permutation process, (x_n, y_n) and (x_{n+1}, y_{n+1}) denote the old and new pixel positions, and N stands for the width or height of a square image. The parameters a, d can be recognized as the secret keys. The application of discrete Henon map to a gray image 512 × 512 shown in Fig. 1 produced permutated images as demonstrated in Fig. 2. Besides, two other discrete 2-D maps named Standard map [21] and Arnold Cat map [44] are also tested for image permutation, as illustrated in Figs. 4 and3, respectively. By comparison of our experimental results, it