Signal Processing 150 (2018) 233–247

Contents lists available at ScienceDirect

Signal Processing

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

Design of image cipher using life-like cellular automata and chaotic map

Ping Ping*, Jinjie Wu, Yingchi Mao, Feng Xu, Jinyang Fan

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

ARTICLE INFO

Article history:
Received 26 December 2017
Revised 17 April 2018
Accepted 18 April 2018
Available online 19 April 2018

Keywords:
Image encryption
Two-dimensional Logistic-adjusted-Sine map
Life-like cellular automata
Balanced rule
Weighted histogram

ABSTRACT

Recently, a number of image ciphers using cellular automata (CA) or combined with chaotic maps have been proposed. However, most of them suffer from some intrinsic drawbacks such as small rule space, low diffusion and no explicit classification of CA rules. To overcome these drawbacks, this paper presents a novel image cipher based on Life-like cellular automata and chaos. The proposed image cipher consists of two sub-processes: permutation and substitution. In the permutation, a two-dimensional Logistic-adjusted-Sine map (2D-LASM) with excellent properties is adopted to shuffle the pixel positions. In the substitution, a second-order Life-like CA with a balanced rule is employed. The balanced rules make the distribution of 0 and 1 in Life-like CA gradually be in equilibrium during the process of iteration. Second-order CA can preserve the result of CA after each iteration to obtain the reversibility. Furthermore, to resist chosen-plaintext and known-plaintext attacks, the algorithm controls the initial conditions of 2D-LASM by the key and the weighted histogram of the plain-image. Theoretical analysis and experimental results both show that the proposed scheme has prominent cryptographic performances and can resist the common attacks effectively, which is very suitable for image encryption.

1. Introduction

Nowadays, with the rapid development of information technology, plenty of digital images have been transmitted on the networks, stored in the cloud and shared in mobile phones. These images not only involve personal privacy but also relate to social safety. Therefore, the security of digital images is highly regarded [27] and various image ciphers [1,4–6,14,16,20,37,41,43,45,48] have been proposed. In recent years, two dynamic systems called cellular automata (CA) and chaotic system have been shown to be suitable for image encryption due to their attractive features such as sensitivity to initial condition, random-like dynamical behaviors, and unpredictability of evolution.

Chaos is a non-linear dynamic system which has been widely applied in cryptography [8,9,13,15,19,24,33,39,46]. For one-dimensional (1-D) chaotic maps, such as Logistic map, Sine map and Tent map, their structures and trajectories are very simple, therefore the hardware implementations are relatively easy. For example, Wang et al. [39] utilize 1-D Logistic map to encrypt the R, G, B components of a color image at the same time. In [7], the algorithm uses 1-D Logistic-Sine System (LSS) derived from Logistic map and Sine map to generate pseudo-random sequences for block permutation and block diffusion. However, as the chaotic signal estimation techniques develops [21,25], the encryption schemes using 1-D chaotic maps are risky to be broken [2,17,18]. Once little information leaks out, chaotic orbits and initial states may be estimated because of simple chaotic behavior and small key space. On the other hand, high-dimensional chaotic maps, such as Intertwining Logistic map [33,46] and Lorenz system, have more variables and parameters. Their structures are more complex, and orbits are harder to be predicted. In particular, high-dimensional hyper-chaotic systems have more than one Lyapunov exponents, with more complex behaviors. In [13], Gao and Chen propose a hyper-chaotic system for image encryption with excellent performances and large key space. However, it is difficult to resist chosen-plaintext and known-plaintext attacks [32] due to the weakness of the encryption structure that lack of correlation between the keystream generation and the plain-image. In [41], Wang et al. add a nonlinear controller on the basis of Lorenz system, making the chaotic map become a four-dimensional hyper-chaotic map. Although high-dimensional chaotic system has outstanding performance, it requires a high computational overhead, which increases the entire time of image encryption.

CA is a discrete dynamical system. It possesses a unique advantage in the field of image encryption thanks to its simple regular structure, local interaction, random-like behavior and massive parallelism [34]. It was first introduced into the cryptography by Wol-

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

https://doi.org/10.1016/j.sigpro.2018.04.018
0165-1684/

fram for stream cipher [42]. Since then, many scholars have began to study the application of CA to image cryptosystems [1,3,12,28–30,30,40]. A parallel block-based image cipher with reversible CA is proposed in [23]. It applies the 1-D CA to encrypt the same image by multiple processes running independently on bit-level. In [44], Yang et al. put forward quantum gray-scale image encryption using 1-D quantum CA. However, since the process of evolution is performed on one-dimensional level, the rule space is relatively small, and the diffusion degree is quite low. A 2-D CA named "Game of Life" is applied to scramble the image in [37], but the scrambling effect is not satisfactory, since the scrambled image contains obvious texture features of the original image. In [38], Wang et al. use reversible CA combined with chaotic map to encrypt image. The two initial configurations of 2-D CA are constructed by 4 higher bits of the permuted image and the chaotic map, respectively. Although the algorithm can save the time of encryption, an additional storage space is required to record extra information to ensure that two initial configurations can be used in the decryption phase. In [36], Souyah et al. design an image encryption scheme based on chaotic-memory CA. The pixel values are changed sequentially by means of chaotic system, followed by fourth-order CA associated with the mechanism of quadtree decomposition to further diffuse the image in the substitution stage. Through the above discussion, it can be seen that most CA-based image ciphers adopt the reversible 2-D CA with arbitrary rules, which makes larger key space and higher diffusion degree. However, different local rules of CA produce different evolution properties. Some of them exhibit fixed or periodic structures, while others exhibit random or chaotic aperiodic behaviors. Therefore, the choice of local rules need to be further considered.

It is necessary to establish the association between the cryptosystem and the plain-image in order to make the scheme have an immunity against chosen-plaintext and known-plaintext attacks. In [7], the initial conditions of the chaotic system is calculated by a hash function called SHA256 to make keystream dependent on the plain-image. However, the secret keys are different when different plain-images are encrypted. Thus, they must be transmitted to receivers every time. Not only does the network transmission costs increase, but also the keys are exposed to the risk of being intercepted. In [46], pre-modular operation is proposed at the beginning of encryption and a self-adaptive scheme is designed as a remedy after confusion. The initial values and control parameters are updated by the summation of all pixels in the preprocessed images. However, two different locations of pixels still can be found. When their values are changed at the same time, the summation of all pixels remains unchanged.

To overcome the above matters, this paper proposes a novel image cipher based on reversible Life-like cellular automata (Life-like CA) with a balanced rule combined with chaotic map. In order to obtain high chaotic performances and low computational costs, this paper adopts a two-dimensional Logistic-adjusted-Sine map (2D-LASM). Compared with other 2-D chaotic systems, it has a wider range of chaos and can exhibit hyper-chaotic characteristics. To solve the problems of low diffusion degree in 1-D CA and no explicit classification of rules in 2-D CA, a second-order Life-like CA with balanced rule is proposed. In the substitution stage, the permuted image is transformed into two square binary matrices with the same size, and then the Life-like CA is employed for diffusion. The second-order CA can preserve the result of each iteration to ensure that the scheme has no loss of resolution and obtains the reversibility. Different Life-like rules show different evolution performances. Therefore, balanced rules are selected from the rule space, which can make Life-like CA in equilibrium, that is, in the cell space, 0 and 1 are approximately equal in number and relatively uniform in distribution. In order to withstand chosen-plaintext and known-plaintext attacks, the proposed scheme makes the initial values and control parameter of the 2D-LASM controlled by the key as well as the weighted histogram of the plain-image. Thus, the keystream generated by chaos will be completely different when any one bit is changed in the plain-image. The simulation results and security analyses show that the proposed algorithm has excellent performances in cryptography, and strong capability against various attacks.

The rest of this paper is organized as follows. In Section 2, 2D-LASM and reversible Life-like CA with balanced rules are introduced. Then, in Section 3, the structure of the image encryption algorithm is described in detail. To verify the performance, experimental results and security analyses are shown in Sections 4. At the end, Sections 5 concludes the paper.

2. Preliminaries

2.1. Two-dimensional Logistic-adjusted-Sine map

Logistic map and Sine map are classical nonlinear discrete-time dynamical systems, often used in the field of cryptography. They are defined by Eq. (1) and (2), respectively.

$$x_{i+1} = 4px_i(1 - x_i), \tag{1}$$

$$x_{i+1} = s\sin(\pi x_i), \tag{2}$$

p and s are parameters. When $p \in [0.89, 1]$ and $s \in [0.87, 1]$, Logistic map and Sine map are chaotic. Their bifurcation diagrams are shown in Fig. 1. Though the properties including pseudo-random capability, data irrelevance and computation overhead remain well, they have some common shortcomings, such as small key space, uneven distribution of sequences and crackable trajectory. In order to solve the above problems, this paper adopts a chaotic map called 2D-LASM [15] which is defined as following

$$\begin{cases} x_{i+1} = \sin(\pi\mu(y_i + 3)x_i(1 - x_i)), \\ y_{i+1} = \sin(\pi\mu(x_{i+1} + 3)y_i(1 - y_i)), \end{cases} \tag{3}$$

where μ is a parameter. 2D-LASM is derived from Logistic map and Sine map to obtain more complex structure and larger key space.

Fig. 2 shows that the trajectory of 2D-LASM distributes in the whole region of the 2-D phase plane, which means that 2D-LASM has better ergodicity and the generated sequences are more random.

The Lyapunov exponent (LE) is an important indictor to evaluate chaotic behavior of a dynamical system [35]. A positive LE denotes no matter how close the two initial trajectories are, they exponentially separate with time in the phase plane. In other words, a dynamical system with a positive LE can behave chaos. For multi-dimensional dynamical system, the trajectories can diverge in several dimensions if it has more than one positive LE. In this case, hyper-chaotic behavior appears. According to the method proposed by Ramasubramanian and Sriram [31], 2D-LASM has chaos when $\mu \in [0.37, 0.3] \bigcup [0.4, 0.42] \bigcup [0.44, 0.93]$, and behaves hyper-chaos when $\mu \in [0.44, 0.93]$. Therefore, 2D-LASM is more sensitive to initial conditions. Its structure is more complex and its trajectory is more difficult to be predicted.

2.2. Reversible life-like CA with balanced rules

2.2.1. Life-like CA

Life-like CA is an abstract dynamic system [11,22]. It is described as a 2-D lattice composed of cells with discrete and finite states. It evolutes synchronously at discrete time steps in accordance with the given local rules. The Life-like CA can be defined as $CA = \{C, S, V, f\}$: