Signal Processing 105 (2014) 419–429

Contents lists available at ScienceDirect

Signal Processing

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

# Image encryption based on non-affine and balanced cellular automata

Ping Ping*, Feng Xu, Zhi-Jian Wang

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

ARTICLE INFO

*Article history:*
Received 10 January 2014
Received in revised form
19 May 2014
Accepted 24 June 2014
Available online 1 July 2014

*Keywords:*
Image encryption
Cellular automaton
Non-affine
Balanced

ABSTRACT

On the basis of the analysis and classification of the 256 elementary cellular automata, a kind of non-affine and balanced cellular automata with complex behavior are used as basic blocks in an image encryption scheme. In this scheme, the diffusion operation is performed by the local interaction among cells, while the confusion operation is achieved by the nonlinear and balanced rules applied to cells. As a result, confusion and diffusion are well integrated. Experimental results show that the proposed image encryption scheme has a lot of characteristics, including large key space, low correlation of adjacent cipher pixels, and high sensitivity to the plaintext and key, which can effectively protect the security of the encrypted image.



## 1. Introduction

With the rapid development in network communication, multimedia and cloud computing technology, images can not only be transmitted and published over the Internet, but also be stored in a third party such as Amazon Simple Storage Service (Amazon S3). Protection of images against illegal copying and distribution has become a challenge. Consequently, various image encryption schemes have been proposed as encryption is one of the basic methods of ensuring information security. They include chaos-based methods [1–3], SCAN-based methods [4,5], random grids-based methods [6,7], Fourier Transform-based methods [8,9] and so on. In recent years, cellular automaton (CA) has also been introduced to image security [10–13] thanks to its simple regular structure, local interaction, random-like behavior and massive parallelism. According to the reversibility of CA's global function, CA-based image encryption schemes are able to be categorized into two classes: those based on reversible CA and those based on irreversible CA.

In the case of irreversible CA, Martín [14] has proposed a stream image cipher in which one-time pseudo-random key stream sequence has been generated using a 1-D hybrid CA. Then, Chen et al. [15–17] have developed several image encryption schemes based on 2-D CAs. The kernel of these schemes is the pixel substitution controlled by pseudo-random number sequence, which is generated from a 2-D recursive CA. Recently, a well-known 2-D CA called "Game of Life" is applied to design image ciphers in [18] and [19]. These studies mentioned above share a common feature that CA only act as a pseudo-random number generator (PRNG) in a cipher. Therefore, the security of image encryption system depend on the quality of the CA-based PRNG, which is not secure enough to withstand a powerful cryptographic attack. For example, Li and Lo [20] analyze the security of the CA-based image ciphers in [15,16] and point out that it is insensitive to the plain image and can be easily broken with a chosen-plaintext attack.

In the case of reversible CA, information is preserved during the forward iteration. With this property, reversible

* Corresponding author. Tel.: +86 2587160901.
*E-mail address:* pingpingnjust@163.com (P. Ping).

http://dx.doi.org/10.1016/j.sigpro.2014.06.020
0165-1684/

CA can be made full use of in cryptosystems in a most natural way: the plaintext is coded as an initial configuration of a CA. The CA rule is the key and the final configuration, obtained by forward iteration of the CA for fixed time steps, is the ciphertext. The receiver of the ciphertext, who knows the secret rule, is able to recover the plaintext by backward iteration of the same CA. However, it is proved that there are few reversible rules for 1-D CA and there is no effective procedure for deciding whether or not an arbitrary 2-D CA is invertible [21]. Consequently, it seems to lack any appeal or promise for applying reversible CA to cryptosystems. In order to solve this problem, many researchers attempt to construct a rich variety of reversible CA with certain desirable features rather than spend an inordinate amount of resources on search for reversible CA. For instance, a kind of reversible memory CA are suggested and employed to design image security systems [22–26]. In [22], Chai et al. use a reversible second-order CA to encryption messages and images. The secret key is composed of the local rules, the number of iteration and the input vector sequence. This cryptosystem is featured by its large key space and high speed. Nevertheless, the problem with this approach is that not every CA rule can make sure that CA exhibit random and complex behavior which performs good confusion property. Thus, the quality of encryption varies significantly depending on which rule is chosen. There may exist all kinds of weak keys and even invalid keys in this image encryption system. In [23], the above memory CA has been extended to K-order memory CA and rules 90, 105, 165, 150 have been applied to obtain good confusion property. Although this scheme has no loss of resolution, it is cryptographically weak as it depends on affine rules. Recently, Chatzichristofis et al. [12] have designed an image encryption algorithm based on a periodic attribute of the XOR operation when applied to a 2-D CA rule. It is well known that nonlinear components are essential to every strong cryptographic primitive. But, the rule of 2-D CA adopted in [12] is a linear one in which only XOR logic is involved.

To further enhance the security of CA-based image ciphers, we present a novel image encryption scheme which combines both reversible and irreversible CA. In this scheme, the reversible CA is responsible for confusion and diffusion processes, while the irreversible CA is used to generate pseudo-random key stream sequence. Besides, unlike many CA-based ciphers using linear or affine rules, a special kind of non-affine and balanced rules are adopted for CA to achieve prominent confusion and diffusion properties. The security and performance analyses of the proposed image encryption have been performed using the histograms, statistical tests, correlation coefficients, key sensitivity analysis, and differential analysis. Results demonstrate that our scheme is robust and secure and can be used for the secure image and video communication applications.

The rest of this paper is organized as follows: in Section 2 the basic theory about cellular automaton is presented and a kind of non-affine and balance rules are introduced. Section 3 describes the proposed images encryption algorithm using reversible and irreversible cellular automata. 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.

## 2. Preliminaries

### 2.1. 1-D CA with non-affine and balanced rules

Cellular automaton is an abstract dynamical system in which state, space and time are discrete. A 1-D CA is defined as 1-D lattice of cells, each of which can take a finite number of discrete states, updated synchronously in discrete time steps according to a local rule. Let $s_i^t$ denotes the state of $i$-cell at time step $t$ and $s_i^t \in \{0,1\}$. Then, the local rule of the 1-D boolean CA with radius $r$ has the following form:

$$s_i^{t+1} = f(s_{i-r}^t, \ldots, s_i^t, \ldots, s_{i+r}^t), \tag{1}$$

where $f$ is a boolean function that gives the new state of a cell in terms of the current states of all cells in its neighborhood. From Eq. (1), it follows that the local rule of the boolean CA can be expressed in the form of a lookup table by specifying the values in the 2-bit truth table with $2^{2r+1}$ entries. Table 1 shows an example of a lookup table for an elementary CA ($r=1, s \in \{0,1\}$). In this table, the entries are all possible configurations of $s_{i-1}^t s_i^t s_{i+1}^t$ arranged in an ascending order, and the output is the value of $s_i^{t+1}$. So there is a total of $2^8 = 256$ local rules for an elementary CA, each of which is denoted by an integer $D$ called rule number which is defined as follows:

$$D = \sum_{i=0}^{7} 2^i a_i, a_i \in \{0,1\} \tag{2}$$

The set of states of all CA cells at time step $t$ are called the configuration $C^{(t)}$. At each time step, one configuration is transformed into another new configuration by applying the local rule $f$ to every cell of a CA. This transformation can also be defined by a global function, $F: C^{(t)} \to C^{(t+1)}$, which takes configuration $C^{(t)}$ as an input and then results in a successive configuration $C^{(t+1)}$. For the finite size CA, boundary condition is imposed. Values of the boundary cells are usually all zero, periodic or randomly chosen. In this paper, the periodic boundary condition will be taken into account.

**Definition 1.** Let $f: \{0,1\}^{2r+1} \to \{0,1\}$ be a Boolean function, then a rule of a CA is said to be linear when it can be expressed by equation:

$$f(s_{i-r}^t, \ldots, s_i^t, \ldots, s_{i+r}^t) = w_{i-r} \cdot s_{i-r}^t \oplus \ldots \oplus w_i \cdot s_i^t \oplus \ldots \oplus w_{i+r} \cdot s_{i+r}^t, \tag{3}$$

where $w \in \{0,1\}$, $\cdot$ denotes AND operation and $\oplus$ denotes XOR operation.

**Table 1**
Truth table for an elementary CA.

| $s_{i-1}^t s_i^t s_{i+1}^t$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| $s_i^{t+1}$ | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ |