A new image security system based on cellular automata and chaotic systems

Weinan Wang

Jan 2013

Abstract

A novel image encryption scheme based on Cellular Automata and chaotic system is proposed in this paper. The suggested scheme first utilizes the chaotic sequences generated by Standard map to scramble the pixel matrix of plain image. Then according to cryptographic characteristics such as parallel computation and pseudorandom attribute, the pixel values of the scrambled image are transformed. Furthermore, encryption of different pixels depends on each other in order to diffuse the information of plain image. Simulation experiment and security analysis imply that the proposed scheme has a large key space and is sensitive to secret keys and the cipher image has excellent diffusion properties. Hence, the proposed scheme is of high security and can resist exhaustive attack, sensitive attack and chosen-plaintext attack, etc.

1 Introduction

Nowadays with the rapid development of digital communication and computer science, the security of images, videos and other digital products has attracts more attention. And image encryption is different from text encryption due to the properties of high correlation, data redundancy, etc. Hence, traditional ciphers such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) cannot be effective candidates of qualified encryption methods [1]. Researchers therefore proposed a variety of cryptosystems by combining other models such as chaos-based algorithms [2-5], cellular-automata-based algorithms [6-9] and other model-based algorithms [10-13]. Chaotic systems possess the property of high sensitivity to initial values and system parameters, pseudorandomicity and ergodicity and are widely employed in the fields of image encryption research [14-15]. Cellular Automata are a class of temporally and spatially discrete dynamical systems. Due to the advantages of information processing parallelism, ease of realizing and local interactions [16], they have been widely used to construct cryptosystem and have been a hot issue in cryptography. Wang et. al [2011] proposed a novel encryption technique based on rapid dispersion of errors which could generates stream cipher with excellent pseudorandom property. Zhang et. al [2010] presented an encryption scheme based on improved Cellular Automata, which possesses faster encryption speed and decryption speed. The main characteristics can be described as follows: 1. The stream cipher can be obtained through synchronization of the cipher-text; 2. The efficiency of the encryption algorithm is improved by using Cellular Automata. However, some of the proposed encryption algorithms based on Cellular Automata still have weakness and shortcoming including: 1. In the common encryption algorithm, rules of state transition and iteration step t is chosen as secret keys and hence the key space not large enough to resist the exhaustive attack; 2. Cipher text dose not have
high relationship with the plain text and dispersion of keys errors is slow, through which cryptanalyst can obtain the information of the plaintext by the similarity of the cipher text; 3. Most of the CA-based image encryption algorithms change the pixel values only, which lack enough diffusion and confusion property. Therefore, it is very necessary to investigate some practical secure algorithms to overcome the embarrassing situations mentioned above. In this paper we propose a novel image encryption algorithm by combining Cellular Automata and chaotic map. The encryption architecture is originated from the permutation-diffusion process [19]. The state transition rules of Cellular Automata are extracted from the chaotic sequences of standard map. The confusion stage depends on both the secret keys and the plain image. Numerical simulations and theoretical analysis verify the superiority and effectiveness of the suggested encryption scheme. The rest of the paper is organized as follows. In Section 2, standard map and Cellular Automata model is described briefly. Section 3 performs the permutation stage and diffusion stage to lower the relationship between the plain image and cipher image. In Section 4, algorithm performance and simulation results are reported and analyzed. Finally, Section 5 ends the paper with brief conclusions.

2 Preliminaries

The standard map is a kind of chaotic model which possesses diverse dynamical properties and has been analyzed deeply in the field of physics and biochemistry deeply. It can be defined as follows:

\[ x_{i+1} = (x_i + K \sin(y_i)) \mod 2\pi \tag{2.1} \]

\[ y_{i+1} = (y_i + x_{i+1}) \mod 2\pi, \tag{2.2} \]

where, \( x_i, y_i \in (0, 2\pi) \) and \( i = 1, 2, 3, ..., M \times N \), when \( K = 131 \), the system is in chaotic state.

Cellular Automata is a class of dynamical system which consists of three parts: cells, local state transition rules, neighborhood, and discrete lattice structure. And it can be denoted as:

\[ \{Q, Z^d, N, f\}, \tag{2.3} \]

where \( Q \) is the cell which denotes the discrete lattice structure and \( d \) is the dimension of the Cellular Automata which represents the neighborhood vector space; \( f \) is the state transition rule according to which each cell can have evolution.

Definition 2.1. If all the cells of a Cellular Automata have the same state transition rule, then the Cellular Automata is called a uniform Cellular Automata.

Definition 2.2. If all the cells of a Cellular Automata have various state transition rules, then it is called a hybrid Cellular Automata.

A two dimensional Cellular Automata can be regarded as a lattice matrix with the size of \( M \times N \). Let be the center cell, and its neighborhood can be defined as:

\[ N(i, j) = (S_{i-1,j}, S_{i-1,j-1}, S_{i-1,j+1}, S_{i,j}) \tag{2.4} \]

Hence, the state of \( S_{i,j} \) at the \( t \) step is decided by the neighborhood and itself at \( t - 1 \) step.

\[ S_{i,j}^t = f(S_{i-1,j}, S_{i-1,j-1}, S_{i-1,j+1}, S_{i,j}, S_{i,j}) \tag{2.5} \]
Here we propose a novel cryptosystem based on the coupling of Cellular Automata and chaotic system. In the proposed cryptosystem, the state transition rules of each cell are decided by the chaotic sequences, which can guarantee the dynamical uniformity of the two models. For different secret keys of standard map, the cells will have state evolution in a different way. Firstly, we iterate the standard map and the 2D chaotic sequence \( \{x_k, y_k\} \) is obtained. For each iteration round, map \( x_k \) and \( y_k \) into the formula \( m = \text{mod} (m, 1) \). Then a 4-bit sequence \( (b_1 b_2 b_3 b_4)_k \) is generated by the encryption characteristic function \( f(x) \):

\[
 f(x) = \begin{cases} 
 00, & 0 < m \leq 0.25 \\
 01, & 0.25 < m \leq 0.5 \\
 10, & 0.5 < m \leq 0.75 \\
 11, & 0.75 < m \leq 1 
\end{cases}
\]

Next, let \( r \) represent the \( r \)th round of iteration and we can obtain that:

\[
 B_k = \begin{cases} 
 x_k \rightarrow y_k, & \text{mod} (r, 4) = 0 \\
 y_k \rightarrow x_k, & \text{mod} (r, 4) = 1 \\
 x_k \rightarrow y_k, & \text{mod} (r, 4) = 2 \\
 y_k \rightarrow x_k, & \text{mod} (r, 4) = 3 
\end{cases}
\]

Define each four-bit binary number as rule-deciding number, which decides the state transition rules of each cell. We implement the 2D von Neumann type Cellular Automata model. For \( S_{i,j}^t \), we set the evolution as follows:

\[
 S_{i,j}^{t+1} = (b_1 S_{i-1,j}^t) \oplus (b_2 S_{i,j-1}^t) \oplus (b_3 S_{i+1,j}^t) \oplus (b_4 S_{i,j+1}^t) \oplus (S_{i,j}^t) \quad (2.6)
\]

### 3 The proposed encryption algorithm

The encryption scheme proposed in this paper is based on the permutation-diffusion architecture. Firstly, the chaotic sequences generated from the standard map are employed to shuffle the position of the pixel in the plain image. Then gray-level transformation is performed by the cryptosystem construction of Cellular Automata and standard map. The encryption scheme can be described as follows (take a standard gray-level image of size \( M \times N \) as an example). The first step is to generate keys: two encryption keys Key1 and Key2 are generated from the information of the plain image in order to make cipher image more close to the plain image:

\[
 Key1 = \text{mod} \left( \sum_{i=1}^{M/2} \sum_{j=1}^{N} p_{ij}, 256 \right) \quad (3.1)
\]

\[
 Key2 = \text{mod} \left( \sum_{i=M/2}^{M} \sum_{j=1}^{N} p_{ij}, 256 \right), \quad (3.2)
\]

where \( p_{ij} \) is the pixel value whose position is \((i, j)\) in the plain image. The second step is to iterate the standard map then the pseudorandom sequence \( \{x_k, y_k\} \) in the plain image. The second step is to iterate the standard map then the pseudorandom sequence \( \{x_k, y_k\} \) are generated. We scramble the pixel matrix from left to right, top to bottom, by the standard map:

\[
 \begin{align*}
 i' &= (i + j x_k + Key1) \quad \text{mod} \ (M) \\
 j' &= (j + i' y_k + Key2) \quad \text{mod} \ (N)
\end{align*}
\]
where \((i, j)\) denotes the coordinate of the present pixels position and \((i', j')\) is the position that the former will exchange with and hence we can the scrambled matrix \(P\). The third step is to obtain the four-bit random code \((b_1 b_2 b_3 b_4)_k\) and then decide the transition rules of each cell in the Cellular Automata. The last step is to take Cellular Automata at the \(t\) iteration step, the we perform the gray-level transformation:

\[
C(i, j) = \text{mod} \left( \left( P(i, j) \mod (i S_{t}^{i,j} + j S_{t+1}^{i,j'} + P'(i', j'), 256) \right), 256 \right), \quad (3.3)
\]

where \(P(i, j)\) is the pixel value with the corresponding point at \((i, j)\); \(C(i, j)\) denotes its substitution value; \(P'(i', j')\) is the pixel value of \((i', j')\) in the last encryption round; \(S_{i,j}^{t}\) is the state value of the point \((i, j)\) at \(t\) step.

4 Simulation

In the simulation experiments of the proposed encryption algorithm, the secret keys are set, and we take the 2-D von Neumann Cellular Automata model as the experiments model. A standard gray-level image with the size of is taken as the plain image. The experiment is simulated on a PC with 2GB memory and 2.0 GHz CPU in Intel Core 2 Duo, running on C programming language. The simulation results can be seen in Fig.1. Fig.1(a) is plain image Lena and the cipher image is shown in Fig.1(b).

5 Performance and security analysis

The histograms of the plain image and cipher image are shown in Fig.2 (a) and Fig.2 (b), respectively. The two histograms have shown that cipher image is in great difference from the plain image. In the cipher image, the values of pixels are distributed evenly and conceal the information of the plain image well. Furthermore, the cipher image possesses excellent statistical properties. Hence, the proposed encryption scheme can resist statistical attack effectively.

To resist the exhaustive attack effectively, the encryption algorithm should have large enough key space. In the proposed algorithm, the secret keys consist of \(t, x_0, y_0\). If the double precision of each key is \(10^{-16}\) in the standard map, iteration step \(t\) can reach infinity theoretically according to the practical need. Hence, we can see that the proposed algorithm has large enough key space, which means it can resist the exhaustive attack effectively.

To test the key sensitivity of the proposed encryption algorithm, we make a slight change to each secret key and decrypt the cipher image: \(t = 200, x_0 = 1, y_0 = 0.2000000000000001; t = 200, x_0 = 0.1000000000000001, y_0 = 0.2; t = 201, x_0 = 0.1, y_0 = 0.2). The corresponding decrypted images are shown as follows: The decrypted image with the right keys is in Fig. 3(a) and Fig. 3(b), Fig. 3(c) and Fig. 3(d) are the decrypted images with wrong keys. It is obviously seen even if the keys are changed a little, the decrypted image is quite different from the plain image. Hence, the proposed algorithm has high sensitivity to the initial values of secret keys and can defend sensitive attack effectively.

The correlation coefficients are used to test the properties of diffusion in the cipher image. In the plain image adjacent pixels in an image have high correlation and thus a good algorithm is to lower the high correlation. To test the correlation between pixels in the cipher image using the proposed algorithm
from vertical, diagonal and horizontal directions, 1000 pair pixels are chosen randomly from the plain image and cipher image. The correlation coefficients can be calculated as follows:

6 Conclusion

A novel image security system based on 2D Cellular Automata and standard map is proposed in this paper and has achieved excellent encryption effect. Chaotic sequences are utilized to decide the state transition rules of each cell to enhance the pseudorandomicity of the algorithm. Simulation experiments and security analysis indicate that the proposed algorithm is has large enough key space, and the cipher image shows well distribution and excellent confusion and diffusion properties. Furthermore, the proposed algorithms can resist sensitive attacks and exhaustive attack effectively.

References


