Journal of Computers Vol. 31 No. 6, 2020, pp. 155-168
doi:10.3966/199115992020123106013

A Novel Image Encryption Scheme Based on Hyperchaotic Cellular Automaton

Hai-Yan Gu[1*], Wei-Qing Yan[2], Jing-Hui Zhang[2]

[1] Department of information and art design, Shandong Business Institute, YanTai, Shandong, China
friend5643@126.com

[2] School of Computer and Control Engineering, YanTai University, YanTai, Shandong 264003, China

Received 30 September 2019; Revised 7 January 2020; Accepted 1 March 2020

Abstract. As the traditional encryption method is slow and inefficient in image encryption. The image encryption algorithm using low-dimensional chaos is fast. But it is insecure because of the short period and small key space. To overcome this problem, a hyperchaotic cellular automaton image encryption algorithm is proposed. The hyperchaotic system is disturbed by the Logistic map to avoid the degeneration of digitization. A pseudorandom sequence generator is designed to construct the dynamic permutation box *P*-box and dynamic substituted box *S*-box. A novel invertible cellular automaton is constructed to confuse the plaintext. The image is substituted by the dynamic *S*-box firstly. Then it is encrypted by the invertible cellular automaton. Finally, the *P*-box is used to permutate the rows and the cols. The short period of the chaotic system and the limited key space of the cellular automaton are avoided by joining them together, so that the security can be enhanced greatly. The randomness of the pseudorandom sequence is tested. The encryption efficiency, image lossless, key sensitivity and the ability against attacks are simulated and analyzed. The results show that the proposed scheme is more secure and efficient.

Keywords: dynamic S-box, hyperchaotic system, image encryption, invertible cellular automaton, pseudorandom sequence

1 Introduction

With the rapid development of the Internet, a number of high-definition color images need to be transmitted on the network. Usually, the security of the transmitted information is supported by the cryptosystem. However, since the image has the characteristics of large correlation between pixels, high redundancy and requirement of batch processing, the conventional cryptosystem is unsuitable.

Chaotic systems are widely used in image encryption because of the ergodicity, initial value sensitivity and good randomness [1]. Chaotic-based image cryptosystems are more secure, faster and less computational than traditional cryptosystems [2]. However, one-dimensional chaotic-based image cryptosystem has the disadvantages of small key space, low efficiency and low security. To overcome this problem, many high-dimensional chaotic systems have been proposed for image encryption [3-4]. In literature [5-6], Guo and Tong et al. extends the 2D chaotic map to 3D map to improve the speed of encryption. Gao et al. proposed an image cryptosystem based on hyperchaos [7], but it cannot resist the chosen plaintext attack and chosen ciphertext attack. A color image encryption algorithm based on 3D chaos is proposed in literature [8], but it can be broken by the known plaintext attack and chosen plaintext attack. Zhu et al. use the modified chaotic sequence and plaintext as the final key to encrypt the image [9]. But the secret parameters can be recovered by using chosen plaintext attack. Cellular automaton (CA) encryption technology was first proposed by Wolfram in 1986 [10]. Many researchers explored it extensively in the following decades. It has the characteristics that the implementation is simple and parallelizable [11-12], the high randomness and unpredictability of output [13], the

[*] Corresponding Author

interaction between cells is local and the evolution of cells under different rules is global. These properties enable it to be applied to cryptography and achieve efficient and secure performance [14-16]. The cryptosystem based on CA is mainly divided into two categories: reverse iterative encryption and reversible cellular automaton encryption. The reverse iterative encryption has a large key space and high sensitivity. However, the complexity of the system is greatly increased because of the introduction of random numbers in the reverse iteration. It is not suitable for systems with high real-time requirements. The reversible cellular automaton encryption is simple, fast, and efficient. But it only has six kinds of classic reversible cellular automaton. This results in a smaller key space and lower security. Though more reversible cellular automatons are constructed to improve the security, the total number of combinations of the reversible cellular automaton is only 16. It is still insecure when the number of iterations is small.

In conclusion, the pseudorandom sequence generated by chaotic system is suitable for image encryption. But the small key space of low-dimensional chaotic system decreases its security. The key space of higher dimension chaotic system is large enough for the security. However, the limited precision of compute degenerates the randomness of the sequence. Furthermore, the chaos-based image encryption schemes are insecure against chosen-plaintext attack and known plaintext attack. On the other hand, the output of CA is unpredictable and its implement is paralleled highly. But the small key space constrains its applicability. Aiming at these problems, we proposed an image encryption algorithm based on disturbed hybrid hyperchaotic cellular automaton. Since the disturbed hybrid hyperchaotic system has larger key space and less degeneration. This can extend the key space of CA drastically while keeping the unpredictable and high paralleled characters of CA.

The main contributions of this work are as follows: I) A disturbed hybrid hyperchaotic system is proposed. A pseudorandom sequence generator is designed to quantize the hyperchaotic system into pseudrandom sequences. The dynamic P- box and S-box are constructed by using the pseudorandom sequences.II) A novel reversible cellular automaton is designed. III) An image encryption schemes based on hyperchaotic CA is designed. In this scheme, the pixels of the original image are substituted by using S-box. Then the pixels are encrypted by using the reversible cellular automaton. Finally, permute the rows and columns of the output of CA by using P-box. IV) The security and performance of proposed scheme are analyzed.

The remainder of this paper is organized as below: the background and the relate work are introduced in section 2. In section 3, the disturbed hybrid hyperchaotic system and the pseudorandom sequence generator are designed. The dynamic P-box and S-box are constructed. In section 4, the image encryption scheme based on hyperchaotic CA is designed. The security of proposed scheme is analyzed in section 5. Finally, section 6 is the conclusion.

2 Background and Relate Work

Due to the sensitivity to initial parameter and the great randomness, the chaotic system is widely used in image encryption. Many chaotic systems are proposed in the past years. In this section, the classic chaotic systems are introduced.

2.1 Logistic Map

The Logistic map [17] is one of the most useful chaotic systems. Its dynamic behavior can be described by formula (1):

$$x_{i+1} = \mu x_i (1 - x_i). \tag{1}$$

When $x \in (0,1)$ and $\mu \in [0,4]$, Logistic map is chaotic.

2.2 Lorenz System

Lorenz system [18] is a classic 3D chaotic system. Its dynamic behavior is described by formula (2):

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = cx - y - xz. \\ \dot{z} = xy - bz \end{cases} \tag{2}$$

Here, $a,b,c \in R^+$ are the system parameters. The Lorenz system is a 3-dimension system of ordinary differential equations. Both of the second and third equations contain a quadratic nonlinear term. When $a=10, b=8/3$, and $c=28$, the system is chaotic and has a biplane chaotic attractor.

2.3 Chen System

Chen system [19] has a more complexity behavior than Lorenz system. This provides a higher level of security in the cryptosystem based on Chen hyperchaotic system. Chen hyperchaotic system is described as formula (3):

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = (c-a)x - xz + cy. \\ \dot{z} = xy - bz \end{cases} \tag{3}$$

Here, $a, b, c \in R^+$ are the system parameters. When $a=35, b=3$, and $c \in [20, 28.4]$, the system is chaotic.

2.4 Cellular Automaton

CA is a discrete nonlinear system which consists of a grid of cells with a finite number of stats. It is capable of producing chaotic behavior. The cells are evolving under the specified rule with the increasing of time. In one dimensional CA, each cell has two neighbors and each neighbor has two states. Thus, there are 2^3 possible states for three neighboring. Usually, the state of the i^{th} cell at time t denotes as S_i. The state of S_i at time $t+1$ can be obtained by formula (4):

$$S_i^{t+1} = f(S_{i-1}^t, S_i^t, S_{i+1}^t). \tag{4}$$

Here, f is the specified local rule. It is coded by Wolfram in [20]. For example, let $f(111)=0$, $f(110)=0$, $f(101)=0$, $f(100)=1$, $f(011)=1$, $f(010)=1$, $f(001)=1$, $f(000)=0$, then the binary sequence 00011110 is 30 in decimal. Thus, the CA is named as Rule 30 CA.

The CA can be divided into different categories for its different characteristics: the uniform CA using same rule while non-uniform using different rule. If extreme cells of a CA are adjacent to each other, the CA is said to be a periodic boundary CA. Otherwise, it is called Null boundary CA. A CA is additive if the next states of the cells are calculated by using only the rules that EXOR and/or EXNOR logic. On the other hand, if it only use the rules that only have OR-AND logic.

Different image encryption schemes have their own advantages and disadvantages. We can distinguish them as Table 1.

Table 1. Features of different techniques used in image encryption scheme

Methods	Advantages	Disadvantages
Image encryption scheme based on 1D chaotic system	Simple; Higher speed	Small key space; Degeneration of randomness
Image encryption scheme based on 3D chaotic system	Bigger key space; Higher speed	More complexity; Degeneration of randomness
Image encryption scheme based on CA	Higher parallel; Higher randomness	Small key space

From the above, we can see that the image encryption schemes based on chaotic system are insure for their degenerated randomness. The image encryption schemes based on CA are constrained by its small key space. In this work, we disturbed the hypherchaotic system by using Logistic map, so that the degeneration can be avoided. A novel CA rule is designed and is employed to confuse the plaintext furthermore. Thus, the key space of CA can be extended by the hybrid hyperchaotic system greatly.

3 Design of S-box and P-box based on Hyperchaotic System

3.1 Design of the Pseudorandom Generator Based on Hyperchaotic System

The security of image encryption algorithm based on hyperchaos is mainly determined by the randomness of the pseudorandom. In this paper, we design a pseudorandom sequence generator based on the hybrid hyperchaotic system. The Logistic map is used to disturb the hyperchaotic system proposed in [21]. The hyperchaotic system is shown as below:

$$\begin{cases} \dot{x} = a(y-x) + eyz \\ \dot{y} = cx + dy - xz - w \\ \dot{z} = -bz + xy \\ \dot{w} = rw + hy \end{cases}. \tag{5}$$

Here, x, y, z and w are state parameters, a, b, c, d, e, r and h are constant parameters. The system is hyperchaotic when $a = 14$, $b = 43$, $c = -1$, $d = 16$, $e = 4$, $r = -0.07$ and $h = 4.9$.

The process of digitization usually results in a short period. This is caused by the limited computer precision. To solve this problem, a perturbation for the chaotic system is necessary. In this paper, the Logisitic map is introduced to disturb the state parameter x of the hyperchaotic system to avoid the short period problem.

The produce of the pseudorandom sequence generator designed in this work is as follows:

Step 1: Set the initial value of the hyperchaotic system and the Logistic map. Then iterate the hyperchaotic system 1000 times.

Step 2: Discard the first 1000 values of the hyperchaotic system. Take the subsequent 10000 values, which are denoted as x_i, y_i, z_i and w_i.

Step 3: Transform x_i, y_i, z_i and w_i from real number to binary. Shift the fractional part to the left by 12 bits. The formula is shown in formula (6).

$$x_i^{'} = (x_i - floor(x_i)) \times 10^{12}. \tag{6}$$

Here, $floor(x)$ is the maximum integer that smaller than x.

Step 4: Truncate the upper 8 bits of $x_i^{'}$, $y_i^{'}$, $z_i^{'}$ and $w_i^{'}$. Then concatenate them to obtain a key stream, which is shown as formula (7):

$$k_i = x_{i,1}^{'} \cdots x_{i,8}^{'} y_{i,1}^{'} \cdots y_{i,8}^{'} z_{i,1}^{'} \cdots z_{i,8}^{'} w_{i,1}^{'} \cdots w_{i,8}^{'}. \tag{7}$$

Step 5: Determine whether the number of iterations of the hyperchaotic system reaches to 10000. If true, replace x_i with the iterative value of the Logistic map and continue the next iteration. Otherwise, continue the next iteration without disturbing x_i.

In this system, the initial value of the hyperchaotic system is disturbed by Logistic mapping, which can effectively avoid the short period problem. Secondly, the four dimensions of the hyperchaotic sequence are simultaneously quantized so that each real point can be quantized to 32 bits. The efficiency of key generator is high. Therefore, the pseudorandom sequence generator designed in this paper has higher security and key generation speed.

3.2 Construction of Dynamic *P*-box

In the construction of *P*-box, the key block is chosen according to the size of the image. Support that the image size is $m \times n$, that is, there are m rows and n columns. Then a block with length *m*/2 and *n*/2 are selected from the key stream, which are denoted as $K_{r,i}$ and $K_{c,i}$ respectively. The P-box for rows is generated by using $K_{r,i}$ as shown in formula (8):

$$\begin{cases} P_r(i, i+m/2), K_{r,i} = 1 \\ P_r(i,i), K_{r,i} = 0 \end{cases}, i \in \{1, 2, \cdots, m/2\}. \tag{8}$$

Here, $P_r(x, y)$ denotes that exchange the x^{th} row and the y^{th} row. The P-box for columns is generated by using $K_{c,i}$ as shown in formula (9):

$$\begin{cases} P_c(i, i+n/2), K_{c,i} = 1 \\ P_c(i,i), K_{c,i} = 0 \end{cases}, i \in \{1, 2, \cdots, n/2\}. \tag{9}$$

3.3 Construction of Dynamic *S*-box

In this section, the *S*-box is constructed dynamically by using pseudorandom sequences generated in section 3.1. The nonlinear modular operation is used in the S-box to improve the security. The construction of *S*-box and invertible *S*-box is shown in formula (10):

$$\begin{cases} c = ((m)^{-1} \bmod 257 + key) \bmod 256 \\ m = ((c - key) \bmod 256)^{-1} \bmod 257 \end{cases}. \tag{10}$$

Since the ranges of pixel value of the image is [0, 255], each pixel value can be replaced by another value in the range [0, 255] by using formula (10). The substitution operation of proposed *S*-box is faster than the traditional AES *S*-box.

4 Image Encryption Scheme Based on Hyperchaotic Cellular Automaton

4.1 Design of Invertible Cellular Automaton

The construction method of the reversible cellular automaton is first proposed by Wolfram, and its definition is as below:

Definition 1. Reversible Cellular Automaton (RCA): The reversible cellular automaton is a cellular automaton that meets the following condition:

Support that C_0 is an initial configuration of a cellular automaton, the configuration C_n can be obtained by acting the evolution rule f_1 on it for n times. Furthermore, C_n is used as the initial configuration, the configuration C_0 of the cellular automaton can be obtained by acting the evolution rule f_2 on it for *n* times. Then the cellular automaton which corresponding to the evolution rules f_1 and f_2 is a reversible cellular automaton only if $f_1 = f_2$. It can be expressed as formula (11):

$$\begin{cases} C(t+n) = f_1(C(t)) \\ C(t) = f_2(C(t+n)) \end{cases}. \tag{11}$$

Definition 2. Constructed reversible cellular automaton: when the state value C_t of the i^{th} cell at time *t* is determined jointly by the i^{th} cell state of the previous moment which denotes as C_{t-1}, the state value of its *r* neighbor cells and the i^{th} cell state value at time *t-2* which denotes as C_{t-2}. The reversible cellular automaton is constructed. It can be descripted as formula (12):

$$C_i^{t+1} = f(C_{i\text{-}r}^t, C_{i\text{-}r+1}^t, \cdots, C_{i-1}^t, C_i^t, C_{i+1}^t, \cdots, C_{i+r}^t, C_i^{t-1}. \tag{12}$$

Where *r* is the neighbor radius.

In this work, the reversible cellular automaton constructed is based on the elementary cellular automaton. We denote it as *33R*. The neighbor radius *r=2*. The rule of the 33th elementary CA is shown in Table 2.

Table 2. Elementary Cellular Automaton Rules of No. 33

time	state							
t	111	110	101	100	011	010	001	000
t+1	0	0	1	0	0	0	0	1

According to formula (12), the local transformation rule of *33R* can be obtained. The processing is shown in Fig. 1.

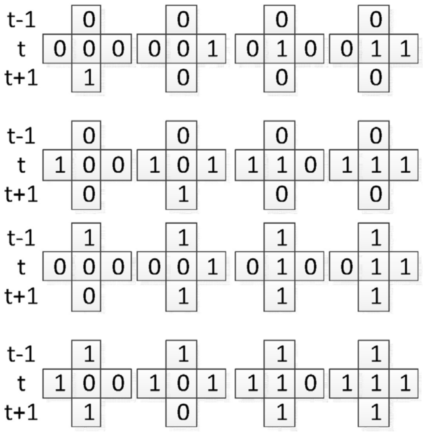

t-1 0 0 0 0
t 0 0 0 0 0 1 0 1 0 0 1 1
t+1 1 0 0 0
t-1 0 0 0 0
t 1 0 0 1 0 1 1 1 0 1 1 1
t+1 0 1 0 0
t-1 1 1 1 1
t 0 0 0 0 0 1 0 1 0 0 1 1
t+1 0 1 1 1
t-1 1 1 1 1
t 1 0 0 1 0 1 1 1 0 1 1 1
t+1 1 0 1 1

Fig. 1. Local transformation rules of the reversible cellular automaton *33R*

The reversibility of the constructed *33R* cellular automaton is proved as below:

Set the two initial states of the shifting cellular automaton to be 000001000000 and 000001100000 respectively. We can obtain cell grid state 110001111111 after 4 times' forward evolution by applying the constructed reversible cellular automaton (RCA) *33R* on it. Then set the state value of this step and the third step to be the initial state. The initial state of the one-dimensional cellular automaton can be obtained by 4 times' backward evolution. The processing is shown in Fig. 2.

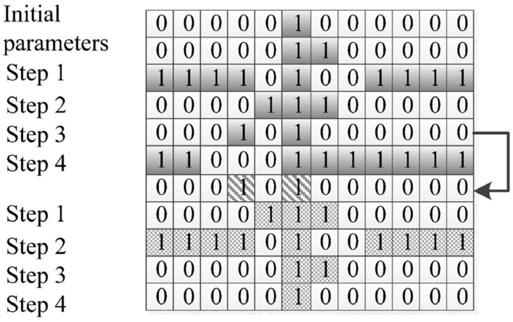

Initial parameters
0 0 0 0 0 1 0 0 0 0 0 0
0 0 0 0 0 1 1 0 0 0 0 0
Step 1 1 1 1 1 0 1 0 0 1 1 1 1
Step 2 0 0 0 0 1 1 1 0 0 0 0 0
Step 3 0 0 0 1 0 1 0 0 0 0 0 0
Step 4 1 1 0 0 0 1 1 1 1 1 1 1
0 0 0 1 0 1 0 0 0 0 0 0
Step 1 0 0 0 0 1 1 1 0 0 0 0 0
Step 2 1 1 1 1 0 1 0 0 1 1 1 1
Step 3 0 0 0 0 0 1 1 0 0 0 0 0
Step 4 0 0 0 0 0 1 0 0 0 0 0 0

Fig. 2. The reversible process of rule *33R*

Thus, the *33R* cellular automaton constructed in this work is reversible.

4.2 Structure of Proposed Image Encryption Scheme

In the image encryption algorithm based on hybrid hyperchaotic cellular automaton, the image is first replaced with *S*-box. Then it is encrypted by the reversible cellular automaton. Finally, permute the rows and columns of the image by *P*-box constructed in section 3.2 and 3.3 correspondingly. The encryption model is shown in Fig. 3.

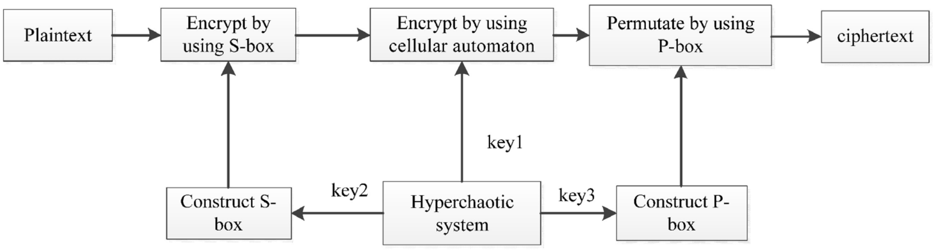


Fig. 3. Encryption model

As shown in Fig. 3, the proposed image encryption scheme consists of encryption and decryption. The pseudorandom sequence generated by the hybrid hyperchaotic system is used as the key. The *P*-box and *S*-box are constructed dynamically with the controlling of the key. The details of the image encryption scheme are described in section 4.3.

4.3 Encryption Algorithm and Decryption Algorithm

The encryption algorithm and decryption algorithm are described as below.

(1) Encryption Algorithm

The encryption algorithm process is descripted as following steps:

Step 1: Convert the plaintext image *M* into $m \times n$ pixel points. Use the *S*-box to perform an alternative operation on the *M*. Support that the plaintext pixels of the image is $M_{i,j}$, then $M1_{i,j} = ((M_{i,j})^{-1} \bmod 257 + K_{i,j})$ $\bmod 256$, where $1 \le i \le m, 1 \le j \le n$, $K_{i,j}$ is the secret key.

Step 2: Obtain a pseudorandom sequence S_0 with length $m \times n \times 8$. Convert the scrambled pixel *M1* into a binary sequence S_1 with length $m \times n \times 8$ in row order. Let S_0 and S_1 to be the initial state variables. Perform encryption operation by using the reversible cellular automaton which designed in 4.1. The neighbor radius is *r=2* and the number of evolution is *n=4*. Thus we can obtain the ciphertext *M2*. The process is shown in Fig. 4.

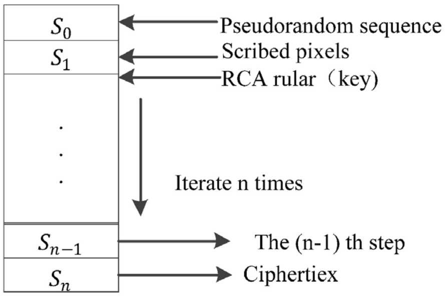


Fig. 4. Cellular automaton encryption process

Step 3: Convert *M2* into $m \times n$ pixel matrix *M3* in row order. The range of pixels is [0, 255].

Step 4: Perform row permutation on *M3* by using *P*-box P_r. Then perform column permutation on it by using *P*-box P_c.

After the above steps, the ciphertext image *C* is obtained.

(2) Decryption algorithm

The decryption algorithm is the inverse of the encryption algorithm. The decryption model is shown in Fig. 5.

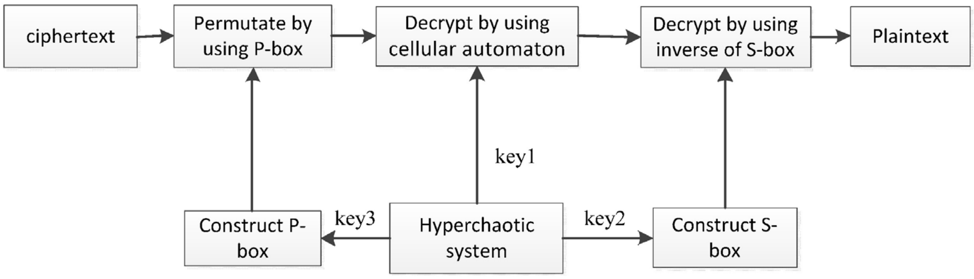


Fig. 5. Decryption model

In the decryption algorithm, we use the inverse of S-box but not S-box. The P-box is as same as it in the encryption. In the decryption process of the cellular automaton, the only difference is the input parameters. Therefore, the decryption speed is much faster than the traditional method. The decryption process is as follows:

Step 1: Convert the ciphertext image *C* into $m \times n$ pixel points. Perform the column permutation on *C* by using the *P*-box P_c and row permutation by using the *P*-box P_r to obtain *C1*.

Step 2: Convert *C1* into $m \times n \times 8$ binary sequence S_n. Use S_n and the result of the $(n-1)^{th}$ step S_{n-1} in the cellular automaton encryption process as the initial state parameters. Perform the backward evolution for *n* times. Then the ciphertext *C2* is obtained.

Step 3: Convert the ciphertext *C2* into $m \times n$ pixel point matrix *C3*. Here, the range of the pixel value is [0, 255].

Step 4: Use the inverse of *S*-box to perform an alternative operation on *C3*. Support that the ciphertext pixel of the image denotes as $C3_{i,j}$, then the plaintext *M* can be obtained from *C3* by using $M = ((C3_{i,j} - K_{i,j}) \bmod 256)^{-1} \bmod 257$.

After the above steps, the plaintext image *M* is recovered.

5 Security Analysis

5.1 Randomness of the Key

The randomness of the key stream is an important indicator to measure the security of the encryption algorithm. The randomness of the pseudorandom sequence obtained by the proposed scheme is tested by using NIST SP 800. We compared the results of proposed scheme with literature [21]. The comparison is shown in Table 3.

Table 3. The comparison of SP 800 22 test for different schemes

Test item	Proposed scheme		Ref [21]	
	P-value	Proportion	P-value	Proportion
Frequency	0.350485	1	0.9558	1
BlockFrequency	0.153763	1	0.3041	0.98
CumulativeSums	0.112089	1	0.1816	1
Runs	0.350485	0.99	0.6163	1
LongestRun	0.249284	0.99	0.5341	0.99
Rank	0.574903	1	0.6787	1
FFT	0.616305	0.99	0.5544	0.99
NonOverlappingTemplate	0.522198	0.99	0.5464	1
OverlappingTemplate	0.798139	1	0.5544	1
Universal	0.56152	1	0.6371	0.99
ApproximateEntropy	0.55442	0.98	0.2133	0.98
RandomExcursions	0.308723	1	0.2357	1
RandomExcursionsVariant	0.225165	1	0.2135	0.98
Serial	0.468485	0.99	0.2622	0.98
LinearComplexity	0.955835	1	0.12962	0.99

It can be seen from Table 2 that the key stream generated by the proposed scheme passed the entire randomness test. Furthermore, there are 9 items whose proportion equals to 1 in proposed scheme while the literature [21] only has 7. Thus the proposed scheme has a high randomness, which can provide higher security for the encryption algorithm.

5.2 Analysis of Encryption Efficiency

The encryption effect test is used to test the visual encryption effect of the picture. In this paper, the image Lena and Cman is selected as the test image. The results are shown in Fig. 6 and Fig. 7.

(a)Original image (b) Encrypted image

Fig. 6. Original image of Lena and encrypted image of Lena

(a) Original image (b) Encrypted image

Fig. 7. Original image of Lena and encrypted image of Cman

It can be seen that the encrypted image is unrecognized at all. Thus the proposed scheme has a perfect encryption effect.

5.3 Analysis of the Image Lossless

Peak Signal-to-Noise Ratio (PSNR) is a common standard used in the measuring of image encryption. Based on the definition of mean error variance (MSE), it describes the mean square error between the processed image and the original image. *MSE* is defined as follows:

$$MSE = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}(P_0(i,j)-P_1(i,j))^2. \quad \textbf{(13)}$$

The *PSNR* is defined by formula (14):

$$PSNR = 10\log_{10}(\frac{L^2}{MSE}). \quad \textbf{(14)}$$

Where L is the maximum possible pixel value of the image, P_0 is the original image and P_1 is the processed image. The image size is denotes as $W \times H$. As each pixel is represented by 8 bits, *L=255*. From equations (13) and (14), it can be seen that if $P_0 = P_1$, then the *PSNR* is infinite or undefined. Because *MSE=0* in this condition. The larger the *PSNR* value, the more similar between the original image and the processed image. Table 4 lists the *PSNR* and *MSE* values of the original image and the encrypted image for the proposed method and the method in literature [8, 22].

Table 4. Comparison of MSE and PSNR of original images and encrypted images using different method

Image	The proposed scheme		Scheme in Ref [22]		Scheme in Ref [8]	
	MSE	*PSNR*	*MSE*	*PSNR*	*MSE*	*PSNR*
Lena	0.0039	72.2302	11.5899	37.49	0.6041	50.32
Peppers	0.0047	70.1285	26.7350	33.86	0.8651	48.76
Baboon	0.0028	74.8932	8.1486	39.02	0.4037	52.07

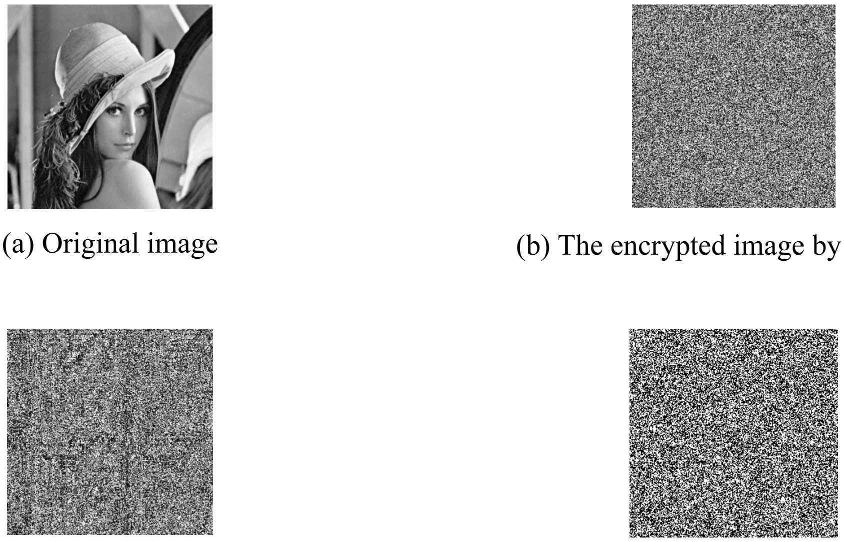
It can be seen that the *MSE* of the proposed scheme is close to 0. This means that there is almost no difference between original image and the encrypted image. Thus the encryption algorithm of this work is approximately lossless.

5.4 Analysis of Key Sensitivity

Since the original image is encrypted by the pseudorandom sequence which generated by the hybrid hyperchaotic system. The sensitivity of the key is an important indicator for measuring the security of the encryption algorithm. The key sensitivity test is divided into two parts: the sensitivity of different keys in encryption and the sensitivity of different keys in decryption.

(1) Sensitivity of different keys in encryption

The sensitivity of different keys in encryption used to measure the relevance of the ciphertext which is encrypted by different keys. The smaller correlation denotes the higher sensitive of the keys. In this work, the Lena image is used for testing. The initial state parameter $x(0)$ is modified with a precision of 10^{-14} to obtain $x(1)$ and $x(2)$. Without changing the other parameters, the pseudorandom sequences k_0, k_1 and k_2 are generated. Then the original image Lena is encrypted by suing these three different keys. The original and the encrypted images are shown in Fig. 8.



(a) Original image

(b) The encrypted image by using k_0

(c) The encrypted image by using k_1

(d) The encrypted image by using k_2

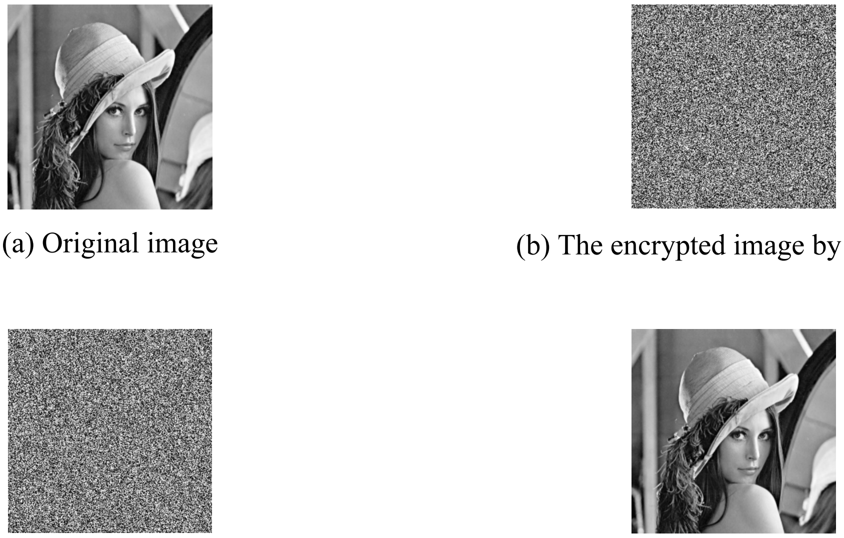
Fig. 8. Comparison of the of original image of Lena with the encrypted images

The ratios of the different pixels between original image and the encrypted images are as below: the ratio of different pixels between Fig. 8(a) and Fig. 8(b) is 99.27%, the ratio of different pixels between Fig. 8(a) and Fig. 8(c) is 99.13%, the ratio of different pixels between Fig. 8(a) and Fig. 8(d) is 99.36%.

From Fig. 8, we can see that the subtle changes in the keys will result in a huge difference between the encrypted images and the original image.

(2) Sensitivity of different keys in decryption

In the sensitivity test of different keys in decryption, the encrypted image is decrypted by using a key that only has a subtle difference from correct key. If the original image cannot be decrypted correctly, the sensitivity of the key is high. In this paper, the key k_0 is used to encrypt the Lena image. The encrypted image is shown in Fig. 9(b). We obtain k_4 by modifying any 1 bit of k_0.Use k_4 to decrypt Fig. 9(b) and obtain Fig. 9(c). The ratio of different pixel between original image and Fig. 9(b) is 99.49%. The ratio of different pixel between original image and Fig. 9(c) is 99.15%. The ratio of different pixel between Fig. 9(b) and Fig. 9(c) is 99.21%.



(a) Original image

(b) The encrypted image by using k_0

(c) The decrypted image by using k_4

(d) The decrypted image by using k_0

Fig. 9. Comparison of the decrypt images with different keys

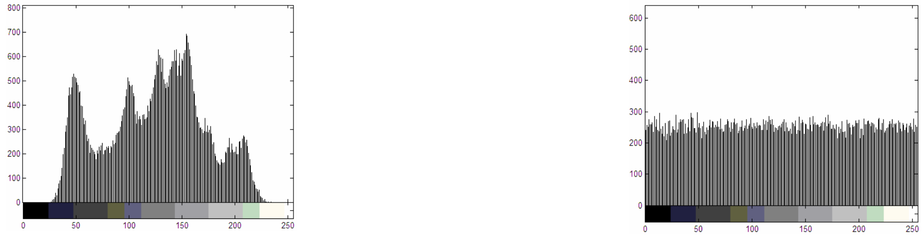
From the above, we can see that the keys with subtle difference will cause completely difference in the encrypted images. Furthermore, the key with slight difference in decryption will result in a completely illegible plaintext. Therefore, the proposed scheme has a higher key sensitivity.

5.5 Statistic Attack Analysis

The statistic attack analysis includes histogram analysis, correlation analysis and information entropy analysis.

(1) Histogram analysis

The histogram of the image describes the gray distribution curve in the image, which is the statistics of the pixel frequency in each luminance space interval. Assuming that the digital image has $W \times H$ pixels whose gradation range is divided into K intervals. Each of the K intervals corresponds to the gradation value of one pixel. The histogram distribution of the encrypted image can hide the information, redundancy of original image. It also does not reveal any relation between the original image and the encrypted image. As the histogram of the encrypted image is evenly distributed, it can resist the histogram analysis attacks. Fig. 10 is the histogram of the original image and the encrypted image.



(a) Histogram of the original image

(b) Histogram of the encrypted image

Fig. 10. Histogram comparison of original image and encrypted image

In Fig. 10, the histogram pixels of the encrypted image are almost evenly distributed. Thus the proposed algorithm can resist the histogram analysis attack.

(2) Correlation analysis of adjacent pixel points

Usually, there is a large correlation between the pixels of the image. If the correlation between adjacent pixels of the encrypted image is low, the encryption algorithm is more secure. The correlation between adjacent pixels can be calculated by using formula (15):

$$r = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\sum_{i=1}^{N}(x_i - \overline{x})\right)^2 \left(\sum_{i=1}^{N}(y_i - \overline{y})\right)^2}}. \tag{15}$$

Where $\overline{x}$ and $\overline{y}$ are the average of the selected pixels. In this paper, the correlation between adjacent pixels of the original image and the encrypted image is analyzed and compared with other schemes. The results are shown in Table 5:

Table 5. The correlation of the original image and the encrypted image

Image	Row correlation	Column correlation	Diagonal correlation
Original image (Lena)	0.9801	0.9657	0.8936
Encrypted image (Lena) by proposed scheme	0.1018	0.0422	0.0309
Encrypted image (Lena) by Ref [22]	0.1257	0.0581	0.0504
Encrypted image (Lena) by Ref [8]	0.1195	0.5132	0.0487

As shown in Table 4, the correlation between adjacent pixels of original image is high. But it is almost irrelevant between adjacent pixels of encrypted image. Further, it is lower than other schemes. Therefore, the proposed scheme has high confusing ability and can resist the statistical analysis attack of adjacent pixel correlation.

(3) Information entropy analysis

Information entropy analysis is used to assess the uncertainty of the system. For a given message *w*, its information entropy is:

$$H(w) = \sum_{i=0}^{2^N - 1} p(w_i)\log_2 \frac{1}{p(w_i)}. \tag{16}$$

Here, *N* is the binary length of w_i. $p(w_i)$ is the probability that the symbol w_i occurs. For random data with 2^N symbols, the ideal value of information entropy is *N*. Therefore, for a ciphertext image *C* with a gray level of 256, the ideal information entropy is 8. In this paper, the information entropy of image Lena is 7.9895. It is very close to the theoretical value. Thus the proposed scheme can resist the entropy attack.

5.6 Known-Plaintext Attack and Chosen-Plaintext Attack

In known-plaintext attack and chosen-plaintext attack, the attackers usually choose special plaintext and make minor changes to observe the changes of ciphertext. Or they choose some plaintext with linear relationship to observe the characteristics of ciphertext. By using this method, they can obtain secret key.

In this work, the analyses show that the proposed scheme is extremely sensitive to plaintext. The ciphertext obtained by changing different pixel of plaintext is almost uncorrelated with each other. In addition, in the encryption process, the *S*-box and *P*-box are constructed dynamically. The ciphertexts are absolutely different even using the same plaintext. Especially, the encryption operations of *S*-box and the reversible cellular automaton are nonlinear operation. This enhances the security against the known-plaintext attack and chosen-plaintext attack while keeping lower complexity.

From the above, we can conclude that the proposed scheme provide high security, efficiency and lower complexity.

6 Conclusions

Aim at the flaw that digitization process of hyperchaotic system causes a degradation of randomness and the key space of low-dimensional reversible cellular automaton is limited, we proposed an image encryption scheme based on hybrid hyperchaotic reversible cellular automaton.

In this work, the disturbed hyperchaotic sequence is quantized into a binary pseudorandom sequence by using the low-order truncation method. The *S*-box and *P*-box are constructed dynamically by using the pseudorandom sequence. A reversible cellular automaton is constructed by using rule 33R. The image pixels are scrambled by using the *S*-box and then encrypted by the reversible cellular automaton. In the encryption process of the reversible cellular automaton, the pseudorandom sequence is used as one parameter so that it extends the key space drastically. Finally, the *P*-box is used to permute the rows and columns of the image pixels. It confused the correlation of the pixels absolutely. Therefore, the ability that resists the statistic attack analysis can be enhanced furthermore. The simulations show that the pseudorandom sequence generated by the proposed scheme has a better randomness. The secret key is sensitive to the initial value and the ciphertext. Hence, the proposed scheme can resist the differential analysis attacks, statistical analysis attacks and known-plaintext attacks efficiently. It is suitable to be used in the massive image encryption. As the future work, the image encryption based on hyperchaotic system and 2D CA can be studied to enhance the security furthermore.

Acknowledgement

This work is support by Youth program of natural science foundation of Shandong province (ZR2017QF006).

Reference

[1] Q.-Z. Lin, K.-W. Wong, J.-Y. Chen, An enhanced variable-length arithmetic coding and encryption scheme using chaotic maps, Journal of Systems & Software 86(5)(2013) 1384-1389.

[2] R. Enayatifar, H.J. Sadaei, A.H. Abdullah, M. Lee, I.F. Isnin, A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automaton, Optics and Lasers in Engineering 71(2015) 33-41.

[3] M. García-Martínez, L.J. Ontañón-García, E. Campos-Cantón, S. Čelikovský, Hyperchaotic encryption based on multi-scroll piecewise linear systems, Applied Mathematics and Computation 270(2015) 413-424.

[4] Q. Liu, P.-Y. Li, M.-C. Zhang, A novel image encryption algorithm based on chaos maps with Markov properties, Communications in Nonlinear Science and Numerical Simulation 20(2)(2015) 506-515.

[5] G.-S. Gu, J. Ling, A fast image encryption method by using chaotic 3D Cat maps, Optik 125(17)(2014)4700-4705.

[6] X.-J. Tong, M.-G. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator, Signal Process 89(4)(2009) 480-491.

[7] T.-G. Gao, Z.-Q. Chen, A new image encryption algo-rithm based on hyper-chaos, Phys. Lett 372(4)(2008) 394-400.

[8] C.-K. Huang, H.-H. Nie, Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282(11)(2009) 2123-2127.

[9] C.-X. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications 285(1)(2012) 29-37.

[10] S. Wolfram, Cryptography with cellular automaton, in: Proc. Advances in Cryptology- CRYPTO '85 Proceedings, 1986.

[11] P. Anghelescu, E. Sofron, C. Rîncu, V. Iana, Programmable cellular automaton based encryption algorithm, Semiconductor Conference 2(2008) 351-354.

[12] P. Anghelescu, Hardware implementation of programmable cellular automaton encryption algorithm, in: Proc. IEEE International Conference on Telecommunication and Signal Processing, 2012.

[13] M. Tardivo Filho, M.A.A. Henriques, New Possibilities for Cellular Automaton in Cryptography, Faculty of Electrical and Computer Engineering University of Campinas Sao Paulo, Brazil, 2011.

[14] H. Bhasin, N. Alam, Applicability of cellular automaton in cryptanalysis, International Journal of Applied Metaheuristic Computing 8(2)(2017)38-48.

[15] R. Bhardwaj, V. Sharma, Effective image encryption technique through 2D cellular automaton, in: Proc. Progress in Intelligent Computing Techniques: Theory, Practice, and Applications, 2018.

[16] S. Roy, N. Bhatia, U.S. Rawat, A novel cryptosystem using cellular automaton, in: Proc. 2017 IEEE International Conference on Communication and Signal Processing, 2018.

[17] P.F. VERHULST, Notice sur la loi que la population suit dans son accroissement, Correspondances Mathematiques et Physiques 10(1838) 113-121.

[18] E.N. Lorenz, Deterministic nonperiodic flow, Journal of the Atmosphere Science 20(2)(1963) 130-141.

[19] G.-R. Chen, T. Ueta, Yet another chaotic attractor, International Journal of Bifurcation and Chaos 9(7)(1999) 1465-1466.

[20] S. Wolfram, Statistical mechanics of cellular automaton, RevMod Phys 55(1983) 60144.

[21] J. Liu, X.-J. Tong, Y. Liu, M. Zhang, J. Ma, A joint encryption and error correction scheme based on chaos and LDPC, Nonlinear Dynamics 93(3)(2018) 1149-1163.

[22] K. Gupta, S. Silakari, Novel approach for fast compressed hybrid color image cryptosystem, Advances in Engineering Software 49(2012) 29-42.