Image encryption using improved Cubic map and Henon map

Yaoqun Xu[*], and *Xinxin* Zhen

School of Computer, Harbin University of Commerce, Harbin 150028, China

Abstract. In this paper, constructing the improved chaotic map which multiplies the output value of the chaotic map by a large value, and subtracts its integer part. Simulation results show that the chaos range of the improved chaotic map is enlarged. The generated chaotic sequence has strong randomness. A double chaotic image encryption algorithm is proposed by combining the improved chaotic maps with the permutation and diffusion encryption structure. The algorithm can reduce the complexity while ensuring the encryption effect. The simulation results show that the encryption algorithm can resist statistical attack and has excellent robustness, and has a good development prospect in information security.

Keywords: Cubic map, Henon map, Image encryption, Security analysis.

1 Introduction

In the era of big data, a large amount of information is transmitted online every day. The image is visual and intuitive, so the number and application range of image transmission are greatly increased. Therefore, the confidentiality and security of image transmission have been widely concerned, and the exploration of efficient and secure image encryption methods has become a hot topic [1]. Chaotic system has the characteristics of initial value sensitivity and randomness, which is similar to cryptography. Therefore, scholars apply chaotic system to image encryption algorithm, which has become a new research direction. According to the dimension, chaotic systems can be divided into two categories: one-dimensional chaotic systems and high-dimensional chaotic systems [2]. One-dimensional chaotic maps are simple in structure and easy to implementation. However, most one-dimensional chaotic maps have small chaos interval, and the generated sequence value distribution has poor discreteness. Therefore, the image encryption algorithm has the problem of small key space and low security. The high dimensional chaotic system improves the security, but increases the algorithm complexity and implementation difficulty [3].

The traditional Cubic map and Henon map are improved in this paper. The chaos range of the improved chaotic map is enlarged obviously, and the output sequence values are evenly distributed with excellent randomness. An image encryption algorithm based on permutation

[*] Corresponding author: xuyq@hrbcu.edu.cn

and diffusion is designed by using the chaotic sequence generated by improved chaotic maps. The simulation results show that the algorithm can resist attack and improve the security.

2 Chaos map

2.1 Cubic map

Cubic map [4] is a kind of simple chaotic dynamics model, and the mathematical formula is:

$$x_{n+1} = F(\mu, x_n) = \mu \times x_n^3 - (1-\mu) \times x_n \tag{1}$$

The bifurcation diagram of Cubic map Fig. 1(a) depicts the influence of the value of μ on the iteration process. When $\mu \in [3.2,4]$, the dynamical system is chaotic at $(-1,1)$.

2.2 Henon map

Henon map is a classical two-dimensional discrete chaotic map with the following equations:

$$\begin{cases} x_{n+1} = 1 + y_n - a x_n^2 \\ y_{n+1} = b x_n \end{cases} \tag{2}$$

The bifurcation diagram of x component of Henon map is shown in Fig.1(c). It can be seen from the Fig.1(c) that Henon map has narrow chaos interval and simple chaotic orbit.

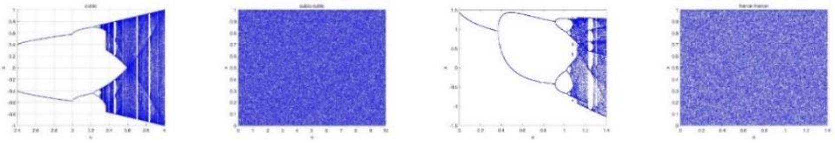
3 Improved chaotic map

3.1 Improved Cubic map

In order to overcome the problem of narrow parameter interval of traditional Cubic map. Use the framework proposed by [5], an improved Cubic chaotic map is proposed in this paper, and the mathematical expression is shown as follows:

$$x_{n+1} = (\mu \times x_n^3 - (1-\mu)x_n) \times 2^{14} - floor((\mu \times x_n^3 - (1-\mu)x_n) \times 2^{14}) \tag{3}$$

The bifurcation diagram of the improved Cubic map is shown in Fig. 1(b).The improved Cubic map expands the parameter range of μ when the model is in the chaotic state.



(a) (b) (c) (d)

Fig. 1. The bifurcation diagram of the (a) Cubic map. (b) Improved Cubic map. (c) Henon map. (d) Improved Henon map.

3.2 Randomness test of time series of improved Cubic map

In order to verify the randomness of improved Cubic map, the international standard NIST test is adopted in this paper. NIST needs to run 15 tests, and at the end of each test comes up with a p-value [6]. When p-value>0.01 indicates that the test passes. Formulas (4-5) is used to process the generated time series. The test results of the Table 1 shows that the time series generated by the model passes the NIST test and can be used in image encryption.

$$s_i = (10^{10} \times x_i)\ mod\ 1 \tag{4}$$

$$y_i = \begin{cases} 0, & 0 \le s_i < 0.5 \\ 1, & 0.5 \le s_i < 1 \end{cases} \tag{5}$$

Table 1. Test result of random sequence.

	Subset	p-value		Subset	p-value
1	Frequency	0.739918	9	OverlappingTemplate	0.350485
2	Block Frequency	0.122325	10	Universal	0.122325
3	Cumulative Sums	0.911413	11	ApproximateEntropy	0.739918
4	Runs	0.534146	12	RandomExcursions	0.818417
5	LongsetRun	0.350485	13	RandomExcursionsVariant	0.445605
6	Rank	0.739918	14	Serial	0.350485
7	FFT	0.739918	15	Linear Complexity	0.213309
8	NonOverlappingTemplate	0.911413			

3.3 Improved Henon map

The mathematical formula of the improved Henon map is as follows:

$$\begin{cases} x_{n+1} = (1 + y_n - ax_n^2) \times 2^{14} - floor((1 + y_n - ax_n^2) \times 2^{14}) \\ y_{n+1} = bx_n \times 2^{14} - floor(bx_n \times 2^{14}) \end{cases} \tag{6}$$

The bifurcation diagram of the improved Henon map is shown in Fig. 1(d). The improved Henon map has improvement in the chaotic region and the scope of parameter influence.

3.4 Randomness test of time series of improved Henon map

The randomness of the time series generated by the improved Henon Map was analyzed by NIST. The results are shown in Table 2.

Table 2. Test result of random sequence.

	Subset	p-value		Subset	p-value
1	Frequency	0.739918	9	OverlappingTemplate	0.739918
2	Block Frequency	0.739918	10	Universal	0.745406
3	Cumulative Sums	0.534146	11	ApproximateEntropy	0.534146
4	Runs	0.213309	12	RandomExcursions	0.779684
5	LongsetRun	0.911413	13	RandomExcursionsVariant	0.681691
6	Rank	0.350485	14	Serial	0.534146
7	FFT	0.739918	15	Linear Complexity	0.601620
8	NonOverlappingTemplate	0.991468			

4 Image encryption

Firstly, read image A of size $M \times N$.

Secondly, two groups of chaotic time series $\{x_M\}$ and $\{y_N\}$ were generated by changing the initial value and using the improved Cubic map to permutate the image. $\{x_M\}$ and $\{y_N\}$ are processed by formula (7) and (8), new sequences a and b are obtained.

$$a = floor(x_i M) + 1 \tag{7}$$

$$b = floor(y_i N) + 1 \tag{8}$$

Thirdly, transpose the row and column positions of the image according to the permutate matrix composed of sequence a and b, and get the permutated image.

Fourthly, improved Henon map is used to generate two chaotic sequences $\{x_{M\times N}\}$ and $\{y_{M\times N}\}$ by iterating $M \times N$ with different initial values.

Fifthly, take the pixel value in the permutated image and set the serial number of the point as n. Use formulas (9) to process sequences $\{x_{M\times N}\}$ and $\{y_{M\times N}\}$. If n is odd, the encryption key is constructed using sequence $\{x_{M\times N}\}$, otherwise sequence $\{y_{M\times N}\}$ is used.

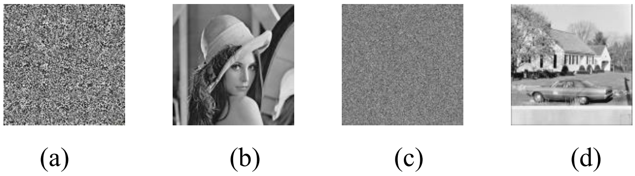
$$key(n) = mod(floor(s(n) \times 10^{15}),256) \tag{9}$$

Sixthly, xor operation between pixel value in permutated image and encryption key value to obtain the encrypted pixel value. After all pixels are operated, the encrypted image $A'(i,j)$ is obtained. The decryption process is the reverse of the above encryption process.

5 Experimental results and security analysis

5.1 Simulation result

Matlab is used to conduct simulation experiments on the image, and the obtained encryption results are shown in Fig. 2. The encrypted image cannot obtain any information.



(a) (b) (c) (d)

Fig. 2. Lena (a) Encrypted image. (b) Decrypted image. House. (c) Encrypted image. (d) Decrypted.

5.2 Information entropy

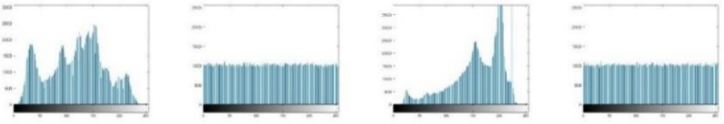
Information entropy can analyze the uncertainty of image. The mathematical formula is:

$$H(x) = -\sum_{i=0}^{n} p(x_i)\, log_2\, p\,(x_i) \tag{10}$$

The information entropy of Lena's encrypted image is 7.9993, which is close to the theoretical value. It indicates that the encrypted image can resist statistical analysis.

5.3 Histogram analysis

Histogram analyzes the distribution of pixel values in an image [7]. Fig. 3 shows the histogram before and after encryption. The pixel values in the encrypted image are evenly distributed. This means that image information cannot be collected using statistical analysis.

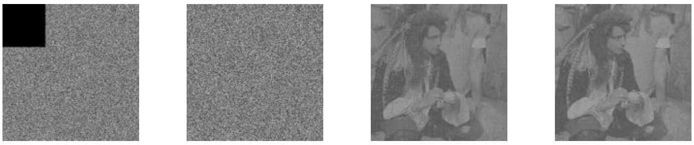


(a) (b) (c) (d)

Fig. 3. Lena (a) Plain image. (b) Encrypted image. House (c) Plain image. (d) Encrypted image.

5.4 Data loss and noise attack

Some pixel values in the encrypted image are set to 0 to simulate data loss dur. Add noise to the encrypted image to simulate the attack. As can be seen from the Fig. 4, the resolution of the decrypted image is reduced. However, the effective information can still be recognized, which proves that the algorithm can resist clipping and noise attack well.



(a) (b) (c) (d)

Fig. 4. (a) The encrypted image with 10% data loss. (b) The encrypted image added with 10% noise. (b) The decrypted image of (a). (e) The decrypted image of (b).

6 Conclusion

To overcome the defects of traditional Cubic map and Henon map, improved chaotic maps are proposed. The improved chaotic map has a wider chaotic interval and the sequence values are evenly distributed. The chaotic sequence generated by improved chaotic maps is used to encrypt the image through the structure of permutation and diffusion. The security of the algorithm is proved by analyzing the simulation results.

This work was funded by Nature Science Foundation of Heilongjiang, grant number (LH2021F035).

References

1. Y. Zhang, The unified image encryption algorithm based on chaos and Cubic S-Box, J. Information Sciences, 450(2108)361-377.
2. K. Noura, S. Amany, A. Mahmoud, An efficient color/grayscale image encryption scheme based on hybrid chaotic maps, J. Optics and Laser Technology, 143(2021).
3. Q. Xu, K. S, C. C, C. Z, A fast image encryption algorithm based on compressive sensing and hyperchaotic map, J. Optics and Lasers in Engineering, 121(2019)203-214.
4. J. Feng, J. Zhang, X. Zhu, W. Lian, A novel chaos optimization algorithm, J. Multimedia Tools and Applications, 76(2017)7405-17436.
5. C. Pak, L. Huang. A new color image encryption using combination of the 1D chaotic map, J. Signal Processing, 138(2017)129-137.
6. I. Yasser, F. Khalifa, A. Mohamed, A.S. Samrah, O. Abedinia, New image encryption scheme based on hybrid chaotic maps, J. Complexity, 2020(2020).

7. S. Zhou, P. He, N. Kasabov, A dynamic DNA color image encryption method based on SHA-512, J. Entropy, 22(2020)1091-1113.
8. X. Wang, Z. Li, A color image encryption algorithm based on Hopfield chaotic neural network, J. Optics and Lasers in Engineering, 115(2019**)**107-118.