2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Design Image Encryption Scheme Using Two-dimensional Henon Map

Ping Ping†, Feng Xu†, Xin Lv† and Xuan Liu†

† College of Computer and Information
Hohai University, Nanjing, China
Email: pingpingnjust@163.com, xufeng@hhu.edu.cn, lvxin.gs@163.com, liuxuan6105@126.com

Abstract–In recent years, various image encryption schemes based on the permutation–diffusion architecture have been proposed. Under this architecture, the pixel positions are firstly shuffled by one map in the permutation stage, and then the pixel values are modified sequentially by another map in the diffusion stage. In this paper, 2D Henon maps are employed to all encryption stages including permutation, diffusion, and key stream generation. Unlike the pixels processed one by one in the diffusion stage in most image ciphers, two pixels are processed simultaneously in our scheme. The extensive security analyses have been carried out and the results demonstrate the high security of the proposed scheme.

1. Introduction

Nowadays, security of image has become increasingly important as more and more confidential images are transmitted over public Internet or stored in a third party. In this respect, various image encryption schemes have been proposed as encryption is a simple and direct way to protect private information.

The methods for image encryption can be classified into three categories according to their architecture: permutation-only, diffusion-only and permutation-diffusion. Among them, the permutation-only type image encryption is commonly referred to as a lightweight image cipher. In [1], the authors present a pure image permutation scheme based on bit-level permutation and a single chaos map. In [2], a two-stage bit-level permutation algorithm is proposed using chaotic sequence sorting and Arnold cat map. However, the permutation-only encryption schemes are vulnerable to some powerful attacks. In [3], Li et al. proposed the quantitative cryptanalysis of permutation-only cipher against known/chosen plain-text attack. For the diffusion-only image cipher, Zhu [4] presented a hyperchaotic sequences based image encryption scheme with only two rounds diffusion operation. But, Li et al. [5] re-evaluated the security of [4] and found it can be broken with only one known plain-image. Compared with the former two structures, the permutation-diffusion is the most widely used architecture for image encryption. For example, Zhu et al. [6] presented an image encryption scheme employing the Arnold cat map for bit-level permutation and the logistic map for diffusion. Zhang et al. [7] successfully cryptanalyzed this scheme and developed an improved one.

In this paper, we propose a novel image encryption scheme based on 2D Henon map. The special attributes of the proposed scheme can be summarized as follows: (1) the 2D Henon maps are employed to all encryption stages. In the permutation stage, pixels are shuffled by an invertible discrete Henon map whose scrambling effect is better than Arnold cat map under the same iteration time. In the diffusion stage, unlike pixels processed one by one in most image ciphers, two pixels are processed simultaneously by the discrete Henon map. (2) In the key generation stage, the key stream generated from the classical Henon map is dependent on the plain-image. As a result, different plain images produce distinct key streams which enhance the resistance to chosen-plaintext attack. The security and performance analyses of the proposed image encryption demonstrate that our scheme is robust and secure and can be used for the secure image communication applications.

2. Two-Dimensional Henon Map

The Henon map is a two-dimensional discrete-time dynamical system which was introduced by Michel Henon as a simplified model of the Poincare section for the Lorenz model [8] .The Henon map equation is defined by:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

where x , y are state variables, a , b are two positive control parameters, n is the number of iteration, $n = 0,1,2...$. The Henon map is widely studied in detail for $a = 1.4$ and $b = 0.3$, where the chaotic behavior was found. For classical Henon map, the time is discrete but the state variables x, y are continuous. In order to facilitate the processing of discrete digital images, we define a discrete Henon map as follows

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \mod N \\ y_{n+1} = x_n + c \mod N \end{cases} \tag{2}$$

where $x, y \in \{0,1,2,...,N-1\}$ are discrete state variables, N is the order of digital image matrix. a , c are two control parameters. It is obvious that the discrete Henon map is invertible. The invertible transformation of Henon map is given by

$$\begin{cases} x_n = y_{n+1} - c \mod N \\ y_n = x_{n+1} - 1 + ax_n^2 \mod N \end{cases} \tag{3}$$

3. The Proposed Scheme

In our scheme, the process of encryption contains multiple rounds of permutation-diffusion to guarantee a satisfactory security level [9]. The 2D discrete Henon maps with different parameters are used in both permutation and diffusion stages, while the 2D classical Henon map is used in key generation. In the following section, we explain the one-round permutation and diffusion operation, which can be easily expanded to multiple rounds of permutation-diffusion.

3.1. Image Permutation

The image permutation stage involves following steps:

Step 1: Determine whether the image is square. If the image is not square, we should expand the image to a square one. The expanded image is denoted by P. The size of the expanded image is $N \times N$ pixels. Let (i, j) stand for the position of the pixel, $i, j \in \{0,1,2,...,N-1\}$.

Step 2: For each pixel (i, j), calculate the new address code (i', j') according to the discrete Henon map with parameters a_0, c_0, and then move the pixel (i, j) to (i', j').

Step 3: Repeat step 2 in an output feedback mode until discrete Henon map iterates t_0 times. As a result of iterating, we obtain the final permuted image P'.

3.2. Image diffusion

It is well known that a permutation-only cipher is vulnerable to plaintext or chosen-plaintext attacks [3]. For the security enhancement, diffusion is introduced after the permutation stage so as to alter the pixel values sequentially and make the cipher sensitive to the plaintext. In the diffusion stage of our proposed scheme, two pixels are processed simultaneously, which improves the efficiency of the cryptosystem. The diffusion stage here is on the basis of obtained the permuted image P'. All the pixels of the permuted image are scanned horizontally from the upper left corner to the lower right corner to form a sequence A_1, A_2,…, A_M, if the image is gray, then $M = N^2$, if the image is color, then $M = 3 \times N^2$. The cipher image C in the diffusion stage is calculated as follows:

(1) The first round

Step 1: Let $x_0 \Leftarrow A_1, y_0 \Leftarrow A_2$, the discrete Henon map with parameters a_1, c_1 iterates t_1 times and generates two final states x_{t_1}, y_{t_1}. Then, let $C_1 \Leftarrow x_{t_1}, C_2 \Leftarrow y_{t_1}$.

Step 2: Let $x_0 \Leftarrow (A_3 + C_1) \bmod 256$, $y_0 \Leftarrow (A_4 + C_2) \bmod 256$, the Henon map with parameters a_2, c_2 iterates t_2 times and generates two final states x_{t_2}, y_{t_2}. Then, let $C_3 \Leftarrow x_{t_2}, C_4 \Leftarrow y_{t_2}$.

Keep on doing until

Step M/2: Let $x_0 \Leftarrow (A_{M-1} + C_{M-3}) \bmod 256$, $y_0 \Leftarrow (A_M + C_{M-2}) \bmod 256$, the Henon map with parameters $a_{M/2}, c_{M/2}$ iterates $t_{M/2}$ times and generates two final states $x_{t_{M/2}}, y_{t_{M/2}}$. Then, let $C_{M-1} \Leftarrow x_{t_{M/2}}, C_M \Leftarrow y_{t_{M/2}}$.

(2) The second round

Let $A_1 = C_M$, $A_2 = C_{M-1}$, $A_3 = C_{M-2}$,…, $A_M = C_1$, and then repeat the steps in the first-round diffusion, where the control parameters $a'_1, a'_2, ..., a'_{M/2}$, $c'_1, c'_2, ..., c'_{M/2}$ and iteration time $t'_1, t'_2, ..., t'_{M/2}$ are used.

Finally, we obtain the cipher image by converting the pixel sequence of the second-round diffusion $C_1, C_2, ..., C_M$ into a pixel matrix.

The decryption is similar to image encryption and is a reverse process of the encryption algorithm.

3.3. Key generation

In our scheme, the key generation produces the parameters and iteration times of the discrete Henon map. There are two sets of parameters, denoted by (a_0 , a_1 ,..., $a_{M/2}$, a'_1 ,…, $a'_{M/2}$), (c_0 , c_1 ,..., $c_{M/2}$, c'_1 ,…, $c'_{M/2}$), and one set of iteration time , denoted by (t_0 , t_1 ,..., $t_{M/2}$, t'_1 ,…, $t'_{M/2}$), used for the permutation and diffusion stages. To make the known-plaintext and chosen-plaintext attacks infeasible, we adopt a method proposed in [10] where the keystream is dependent on the plain image. The key generation algorithm is as follows:

Step 1: Calculate the image feature of a plain image P by

$$\alpha = \frac{\sum_{i,j}(P_R(i,j) + P_G(i,j) + P_B(i,j))}{\sum_{i,j}(P_R(i,j) + P_G(i,j) + P_B(i,j))^2}, 0 < \alpha < 1 \quad (4)$$

Step 2: Give the initial conditions x_0 , y_0 of the classical Henon map defined by Eq.(1). Here, parameters $a = 1.4$ and $b = 0.3$.

Step 3: Update the initial conditions x_0 , y_0 using Eq.(5).

$$\begin{cases} x_0 = x_0 \pm (\alpha \times 10^5 - \lceil \alpha \times 10^5 \rceil) \times 10^{-5} \\ y_0 = y_0 \pm (\alpha \times 10^5 - \lceil \alpha \times 10^5 \rceil) \times 10^{-5} \end{cases} \quad (5)$$

where $\lceil x \rceil$ denotes the floor function of x. Here, we choose the $+$ operation if the updated initial condition is still in area; otherwise, the $-$ operation is used instead.

Step 4: iterate Eq.(1) with the updated initial conditions x_0 , y_0 , and get a sequence { x_0 , y_0 , x_1 , y_1 ,…}. Then, select $3 \times (1 + M)$ values from it after removing the former transient values and obtain a sequence { r_1 , r_2 ,…, $r_{3\times(1+M)}$ }.

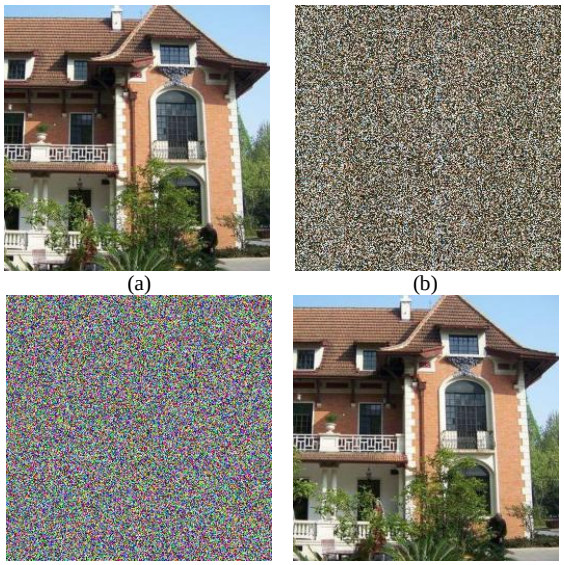
Finally, generate a sequence $\{ r_1', r_2', \ldots, r_{3\times(1+M)}' \}$ using Eq.(6).

$$\begin{cases} r_i' = \lceil r_i \times 10^{15} \rceil \bmod N, \ i = 1,2,...,2M+2 \\ r_i' = (\lceil r_i \times 10^{15} \rceil \bmod 10) + 3, \ i = 2M+3, 2M+4, ..., 3M+3 \end{cases} \quad (6)$$

Step 5: the sequence $\{ r_1', r_2', \ldots, r_{2M+2}' \}$ is sequentially assigned to $\{ a_0, a_1, ..., a_{M/2}, a_1', \ldots, a_{M/2}', c_0, c_1, ..., c_{M/2}, c_1', \ldots, c_{M/2}' \}$, and the sequence $\{ r_{2M+3}', r_{2M+4}', \ldots, r_{3M+3}' \}$ is sequentially assigned to $\{ t_0, t_1, ..., t_{M/2}, t_1', \ldots, t_{M/2}' \}$.

3.4. Simulation Results

Extensive computer simulations have been done with Mathematica 8.0 to examine the validity and robustness of our proposed algorithm. Fig.1(a) shows a color image with 256×256 pixels. By virtue of the encryption algorithm described in section 3, Fig.1(b) shows the intermediate image after the permutation stage while Fig.1(c) is the final cipher image and Fig.1(d) is the decrypted image for recovery of plain image.



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

Figure 1 The simulation results

4. Security and Performance Analysis

4.1. Key Space

The key space refers to the set of all possible keys that can be used in the cipher system. In our proposed image encryption algorithm, the image feature α and the initial values of the classical Henon map x_0, y_0 consist of a external key. If the greatest accuracy is 10^{-15}, the key space is about 10^{30} which is sufficient to prohibit exhaustive attack.

4.2. Correlation Analysis

In general, adjacent pixels of most natural images are highly correlated. An effective encryption scheme should produce the cipher image with sufficiently low correlation of adjacent pixels. To test the correlation between horizontally, vertically, and diagonally adjacent pixels in the image the following procedure is carried out. First, we select N pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient by using the following formulas[11]:

$$C_r = \frac{N \times \sum_{i=0}^{N}(x_i \times y_i) - \sum_{i=0}^{N} x_i \times \sum_{i=0}^{N} y_i}{\sqrt{(N \times \sum_{i=0}^{N} x_i^2 - (\sum_{i=0}^{N} x_i)^2) \times (N \times \sum_{i=0}^{N} y_i^2 - (\sum_{i=0}^{N} y_i)^2)}} \quad (7)$$

where x and y represent gray values of two adjacent pixels in an image. Table 1 shows the correlation coefficients of 20000 pixels pairs adjacent randomly selected. The correlation of plain image is close to 1, whereas the correlation of cipher image is close to 0, therefore, the proposed scheme can resist a statistical attack.

Table 1 The correlation coefficients of adjacent pixels (N=20000)

Image		correlation coefficient		
		Horizontal	Vertical	Diagonal
Plain image Fig.1(a)	R	0.942551	0.860094	0.865182
	G	0.958109	0.863036	0.858106
	B	0.970492	0.875905	0.887813
Cipher image Fig.1(c)	R	-0.004530	0.007052	-0.015839
	G	0.005464	0.005547	0.011636
	B	-0.010408	-0.012224	-0.005633

4.3. Differential Analysis

Generally, the attacker can make a slight change of the plain image, and then observes the change of the result. Thus, he may find out a meaningful relationship between the plain image and the ciphered image. If one minor change in the plain image can cause a significant change in the ciphered image, with respect to diffusion and confusion, then this differential attack would become very inefficient and practically useless. Two common measures named NPCR (number of pixels change rate) and UACI (unified average changing intensity) [12] are usually applied to examine the performance of resisting differential attack.

Tests are carried out with the plain image by using the above-mentioned NPCR and UACI. The average values of NPCR and UACI obtained by the proposed algorithm and another algorithm [11] are shown in Table 2. It is clear that the values of NPCR and UACI produced by these algorithms are very close to the expected values, so these algorithms are good at resisting differential attack.

Table2 NPCR and UACI results of different proposed schemes

	Average NPCR (%)		
Proposed	R :0.996414	G :0.996521	B:0.996521
Ref.[11]	R :0.996262	G :0.996307	B:0.996216
	Average UACI (%)		
Proposed	R :0.335926	G :0.334027	B:0.333906
Ref.[11]	R :0.335115	G :0.332994	B:0.334841

4.4. Key sensitivity

To evaluate the key sensitivity of our scheme, the plain image is encrypted using the test key $\alpha = 4.37149755615800 \times 10^{-8}$, $x_0 = 0.358435602421958$ and $y_0 = 0.605080191163888$. Then, the cipher image obtained is decrypted with the wrong key $\alpha = 4.37149755615800 \times 10^{-8}$, $x_0 = 0.358435602421959$ and $y_0 = 0.605080191163888$. Fig.2 shows the test results, in which Fig.2(a) is decrypted by correct key and Fig.2(b) is decrypted by wrong key. As we can see that even the key is slightly changed, the decrypted image is completely different from the original image. This means that the proposed scheme has a high degree of sensitivity to the key.

(a) (b)

Figure 2 Key sensitivity test

4.5. Chosen-plaintext attack

In the proposed scheme, the parameters of the discrete Henon map used in both permutation and diffusion stages are determined not only by the secret key but also by the plain image. As a result, different plain images produce distinct key streams which enhance the resistance to chosen-plaintext attack.

5. Conclusions

We have designed a novel image encryption scheme based on 2D henon map. Our scheme differs from others in two ways. First, 2D Henon maps are employed to all encryption stages including permutation, diffusion, and key stream generation, which can simplify the hardware implementation. Second, unlike the pixels processed one by one in the diffusion stage in most image ciphers, two pixels are processed simultaneously in our scheme. The results of computer experiments and performance analyses further demonstrate that the scheme can not only achieve good encryption result but also resist against common attacks.

Acknowledgments

This research was supported by the Natural Science Foundation of Jiangsu Province under Grant number BK20130852; the Jiangsu Planned Projects for Postdoctoral Research Funds under No.1401001C; the National Key Technology Research and Development Program of the Ministry of Science and Technology of China under Grant No. 2013BAB06B04; the Key Technology Project of China Huaneng Group under Grant No.HNKJ13-H17-04. The authors would like to thank NOLTA2015 organizing committee members for their fruitful suggestions and comments.

References

[1] G. Ye, “Image scrambling encryption algorithm of pixel bit based on chaos map,” Pattern Recogn. Lett., Vol.331, pp.347-354, 2010.

[2] C. Fu, B. B. Lin, Y. S. Miao, et al., “A novel chaos-based bit-level permutation scheme for digital image encrpytion” Opt. Commun., Vol.284, pp.5415-5423, 2011.

[3] C. Li, K. T. Lo, “Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks,” Signal Process., Vol.91, pp.949-954, 2011.

[4] C. Zhu, “A novel image encryption scheme based on improved hyperchaotic sequences,” Opt. Commun., Vol.285, pp.29-37, 2012

[5] C. Li, Y. Liu, T. Xie, M. Z. Q. Chen, “Breaking a novel image encryption scheme based on improved hyperchaotic sequences,” Nonlinear Dyn., Vol.73, pp.2083-2089, 2013.

[6] Z. L. Zhu, W. Zhang, K. W. Wong, “A chaos-based symmetric image encryption scheme using a bit-level permutation,” Inform. Sciences, Vol.181, pp.1171-1186, 2011.

[7] Y. Q. Zhang, X. Y. Wang, “Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation,” Nonlinear Dyn., Vol.77, pp.687-698, 2014.

[8] M. Henon, “A two-dimensional mapping with a strange attractor,” Commun. Math. Phys., Vol.50, pp.69‑77, 1976.

[9] D. Arroyo, J. Diaz, F. B. Rodriguez, “Cryptanalysis of a one round chaos-based Substitution Permutation Network,” Signal Process., Vol.93, pp.1358-1364, 2013.

[10] X. Huang, G. Ye, “An efficient self-adaptive model for chaotic image encryption algorithm,” Commun. Nonlinear Sci. Numer. Simulat., Vol.19, pp.4094-4104, 2014.

[11] M. A. Murillo-Escobar, C. Cruz-Hernandez, F. Abundiz-Perez, et al., “A RGB image encryption algorithm based on total plain image characteristics and chaos,” Signal Process., Vol.109, pp.119-131, 2015.

[12] X. Wang, H. Zhang, “A color image encryption with heterogeneous bit-permutation and correlated chaos,” Opt. Commun., Vol.342, pp.51-60, 2015