Non-square colour image scrambling based on two-dimensional Sine-Logistic and Hénon map

Siqi Zhou, Feng Xu*, Ping Ping, Zaipeng Xie, Xin Lyu
College of Computer and Information, Hohai University
Nanjing, CHINA, 211100
[e-mail: xufeng@hhu.edu.cn]
*Corresponding author: Feng Xu

Received November 6, 2016; revised March 26, 2017; revised July 17, 2017; accepted August 9, 2017; Published December 31, 2017

Abstract

Image scrambling is an important technology in information hiding, where the Arnold transformation is widely used. Several researchers have proposed the application of Hénon map in square image scrambling, and certain improved technologies require scrambling many times to achieve a good effect without resisting chosen-plaintext attack although it can be directly applied to non-square images. This paper presents a non-square image scrambling algorithm, which can resist chosen-plaintext attack based on a chaotic two-dimensional Sine Logistic modulation map and Hénon map (2D-SLHM). Theoretical analysis and experimental results show that the proposed algorithm has advantages in terms of key space, efficiency, scrambling degree, ability of anti-attack and robustness to noise interference.

Keywords: Image Scrambling, Non-Square, Logistic, Hénon, Chosen-Plaintext Attack

https://doi.org/10.3837/tiis.2017.12.015 **ISSN : 1976-7277**

1. Introduction

As an intuitive tool for describing information, images are widely used in the communication process. With the development of technologies in information and networks, the storage and transmission of information has become increasingly frequent and information security has become an issue. Image scrambling is a technology that transforms a meaningful image to a chaotic image such that the image information cannot be obtained intuitively. As a result, security of information in the process of storage and transmission can be achieved. Image scrambling is widely used in image encryption, information hiding, pre-processing of digital watermarking and certain other fields.

Image scrambling is usually achieved by changing the pixel space position or pixel value, where the former disturbs the order of pixels, and the latter changes the values of each pixel with scrambling algorithms. There are many image scrambling algorithms, such as Arnold transformation[1-5], Magic scrambling[1,4, and 5], Fractal Hilbert curve[5,6], Generalized Gray code transformation[6], Conway game of life[5,7], Tangram algorithm[8], IFS model[8], and Fibonacci transformation[5,9], etc. Among these algorithms, the Arnold transformation is the most classical, and is widely used in information hiding because of its simplicity and feasibility. However, the classic Arnold transformation has several limitations: (1) it can only be applied to square images; (2) it requires multi-iterations to achieve the scrambling effect to a certain degree; (3) the time cost of decryption is expensive because it uses the periodicity of the transformation. Researchers have proposed many improved models to solve these problems [10-13]. To apply the Arnold map to non-square images, Zhao [10] proposed a non-square image scrambling algorithm based on the Arnold map and a simple one-dimensional (1D) Logistic map. Hua [11] proposed a two-dimensional Sine Logistic modulation map (2D-SLMM) to enlarge key space, improve the scrambling efficiency and obtain better chaotic effect. Ping [12] proposed a square image scrambling algorithm using the discrete two-dimensional (2D) Hénon map, the algorithm can improve the scrambling efficiency, achieve high quality scrambling effect in several iterations and decipher the scrambling using inverse transformation. The experimental results in [12] demonstrate better characteristics than using an Arnold map. Kong [13] proposed a new inverse transform algorithm by solving equations based on Arnold map. In [14], the authors proposed an image hashing scheme consists of three main stages, i.e., processing, feature extraction, and hash generation. In the first stage, the original image with arbitrary size are resized to square image by bilinear interpolation. In recent years, chaotic maps have been widely used in image encryption, and have inspired researchers to develop novel image encryption algorithms. These algorithms usually employ one or more chaotic maps for encryption. Because the period of the concatenated torus automorphisms is the total sum of each one's period, Mao [15] proposed a novel chaotic map that concatenates several torus automorphisms and two application schemes. A colour image encryption algorithm based on Logistic chaotic map was proposed in [16], where the chaotic system is used to encrypt the R, G, B components of a color image at the same time and make these three components affect each other. However, the authors in [17] note that in case of a known input and output, the control parameters of the encryption algorithm can be directly deduced. Additionally, because the three basic encryption steps are independent, experimental results show that it can be deciphered by chosen-plaintext attack. Since the transmission of multimedia data became more frequently, the protection of these data has aroused more attention. In [18], the authors proposed a new fragile

watermarking scheme with high-quality recovery capability based on overlapping embedding strategy to protect integrity. To transform an original image into a visually meaningful encrypted one, Bao [19] proposed a new image encryption system (NIES) where the image scrambling algorithm can be used in the pre-encryption process.

The algorithm proposed in this paper is based on 2D-SLMM and Hénon map that is suitable for the scrambling of arbitrary ratio of length to width non-square images and is able to resist chosen-plaintext attack. The purpose of this algorithm is to enlarge the key space, overcome the Arnold transformation periodic defect, make full use of the chaotic characteristics, decrease the complexity of time and space, and resist the chosen-plaintext attack. Experimental results show that the algorithm has a large key space, high scrambling degree, high efficiency and robustness to noise interference.

The rest of this paper is organized as follows. Section 2 introduces the relevant knowledge regarding 2D-SLMM and the 2D Hénon map. In Section 3, the main idea of the proposed algorithm two-dimensional Sine Logistic Hénon Map (2D-SLHM), and the steps of scrambling and deciphering are outlined. Section 4 provides simulation results. Section 5 analyses the performance of the proposed algorithm in key space, chosen-plaintext attack and the noise test, and compares the proposed algorithm with the existing algorithms in time complexity, space complexity and correlation coefficient. Section 6 represents this paper's conclusions and outlines expectations in the image scrambling field.

2. Relevant Knowledge

2.1 1D Chaotic Map

The existing chaotic maps can be divided into two classes: one-dimensional chaotic maps and high-dimensional chaotic maps. The structure and orbit of the 1D chaotic system is simple, and Eqs. (1-2) provide two examples:

$$x_{i+1} = a x_i (1 - x_i) \tag{1}$$
$$x_i + 1 = u \sin(\pi x_i) \tag{2}$$

where a and u are parameters, $a \in [0, 4], u \in [0, 1]$ and $x_{i+1} \in (0, 1)$, the top equation describes the Logistic map and the bottom equation describes the Sine map.

With the development of chaotic signal estimation technologies, the system can be estimated by obtaining small amounts of information, where the parameters and initial values can be predicted easily. Therefore, the encryption algorithm that uses 1D chaotic system suffers from security issues and imposes limitations on its application in the field of security.

2.2 2D-SLMM

High-dimensional chaotic map has a minimum of two parameters that form a complicated structure, and it shows good chaotic performance. Therefore, the prediction of a high-dimensional chaotic map is difficult. To enhance the security of the encryption system, several researchers presented high-dimensional chaotic map models.

Hua [11] proposed 2D-SLMM that combined the Sine map and parameter β to modulate the output of Logistic map to enhance its nonlinearity and randomness as defined by Eq. (3).

$$\begin{cases} x_{i+1} = \alpha(\sin(\pi y_i) + \beta) x_i (1 - x_i) \\ y_{i+1} = \alpha(\sin(\pi x_{i+1}) + \beta) y_i (1 - y_i) \end{cases} \tag{3}$$

where α and β are parameters, and $\alpha \in [0,1]$, $\beta \in [0,3]$. The output values of this model x_{i+1} and y_{i+1} are intertwined that make the orbit difficult to predict.

2.3 Hénon map

The Hénon map is a 2D discrete-time dynamic system which was introduced by Michel Hénon. The Hénon map equations [12] are defined by Eq. (4).

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases} \tag{4}$$

where x, y are state variables, a and b are two positive control parameters, n is the number of iterations. In this model, the time is discrete but the state variables x, y are continuous. The equations [12] of the discrete Hénon map to scramble digital images are defined as Eq. (5).

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \mod N \\ y_{n+1} = bx_n + c \mod N \end{cases} \tag{5}$$

where $x, y \in \{0, 1, 2, ..., N-1\}$ are discrete state variables, N is the order of digital image matrix, a, b, c are control parameters. When $b = 1$, the transformation is invertible as given by Eq. (6).

$$\begin{cases} x_n = y_{n+1} - c \mod N \\ y_n = x_{n+1} - 1 + ax_n^2 \mod N \end{cases} \tag{6}$$

3. 2D-SLHM

3.1 Algorithm idea

Considering the security issue of a 1D Logistic map in [10] and the complexity algorithm in [11], only a portion of the pixels in the non-square plain image are scrambled by 2D-SLMM in this paper. Because of the periodicity, the Arnold transformation cannot directly adopt the inverse transformation to decipher. The algorithm proposed in [12] based on Hénon map can solve this problem, but the algorithm has to expand the image before scrambling a non-square image; hence, it increases the image size. Only after cropping can the original image be obtained in the restoration process, which increases the cost of time and space. In this paper, we construct a virtual square to divide the pixels into two parts. First, we apply the 2D-SLMM transformation to the pixels that are not in the virtual square. Second, the Hénon transformation is applied to the rest of the pixels for two rounds in order to achieve good scrambling effect, the experimental results shown in **Fig. 9**. Finally, all of the pixels are arranged into a non-square image by order to obtain the encrypted image.

3.2 Steps of image scrambling

Step 1: Import image data, get the total pixel number f of the original image, compute the largest integer r, where $r * r \leq f$.

Step 2: Flatten pixels in the image to a sequence, calculate the state values x and y by 2D-SLMM and map them to the position of pixels in the sequence until m different pixels are chosen, where $m = f - r * r$. Delete the pixels in the sequence, and record their position in the matrix *record*, the sum of *x*, *y* to the matrix *s*.

Step 3: Sort the data in matrix s in ascending order, and scramble the chosen m corresponding pixels according to the order to obtain the sequence *q*.
Step 4: Arrange the remainding pixels in a sequence that are not chosen in Step 2 and generate the matrix img that scaled $r * r$ in accordance with the order from left to right, top to bottom.
Step 5: Scramble elements in matrix img by two rounds of Hénon map.
Step 6: Flatten the result of Step 5 and append the pixels to sequence *q*; and subsequently rearrange the sequence to get the final scramble result of the original image.
The algorithm flowchart is shown in **Fig. 1**.

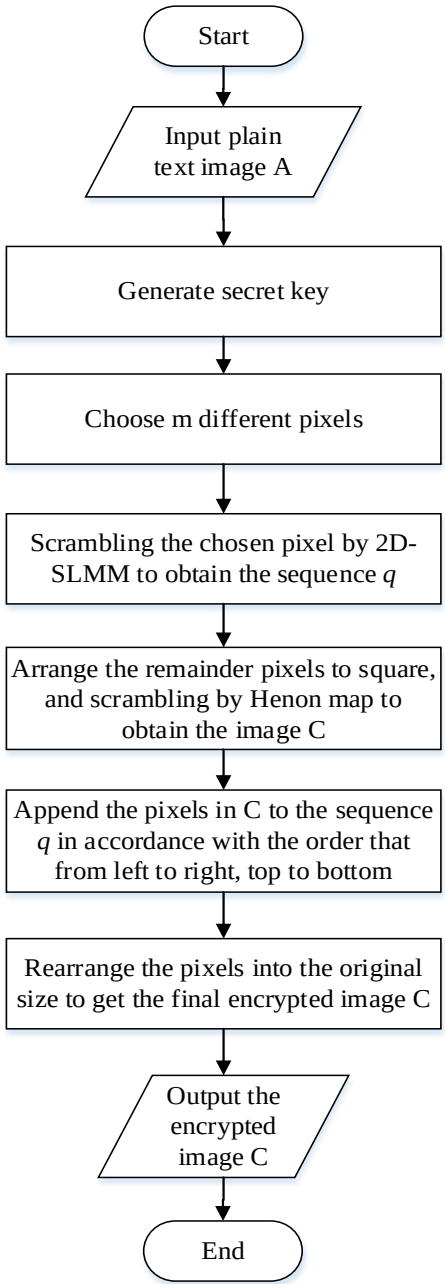


Fig. 1. Algorithm Flowchart

3.3 Steps of image restoration

Step 1: Import image data, obtain the total pixel number f of the original image, compute the largest integer r, where $r * r \leq f$.
Step 2: Flatten the pixel in the image to get the sequence q and set flag = 0 for each position, calculate the state values x, y by 2D-SLMM, until m different pixels are chosen, where $m = f - r * r$. Delete these pixels in q, and record their position in the image to the matrix $record$, the sum of x, y to the matrix s.
Step 3: Sort the data in matrix s in ascending order, then move the m pixels according to the order to the record position and set flag = 1.
Step 4: Scramble the remainder pixels in sequence q by inverse 2 rounds Hénon map, and rearrange them from left to right, top to bottom to the positions that flag = 0.
Step 5: Rearrange q to the size of the original image. Hence, the algorithm yields the original image.

4. Simulation Results

4.1 Secret key

According to [11], the 2D-SLMM map provides a good chaotic effect when β is close to 3. Therefore, we choose $\beta = 3$ in our simulation for the sake of simplicity. Additionally, we choose $b = 1$ according to [12] for deciphering by directly using the inverse operation of Hénon map. Therefore, the secret key consists of x_0, y_0, α, H, G, a, c, t, where x_0, y_0 are initial state variables, α, H, G, a are parameters, and t is the iteration of Hénon map. To resist chosen-plaintext attack, we let the value of c be the sum of values of each pixel. The rest of the secret key is computed by Eq. (7) after randomly generating a binary sequence with 255 bits, where b_i is the ith bit of the binary sequence.

$$x = \frac{\sum_{i=1}^{32} b_i 2^{32-i}}{2^{32}} \tag{7}$$

Next, each initial value is converted to a pre-set range as shown in Eqs. (8).

$$\begin{cases} x_0 = (x_0 + G * H) \mod 1 \\ y_0 = (y_0 + G * H) \mod 1 \\ \alpha = 0.9 + ((\alpha + G * H) \mod 1 \end{cases} \tag{8}$$

4.2 Simulation

The simulation setup is described as follows: Windows 10 (64-bit Professional Edition), Intel Core i7-2630QM CPU @ 2.00 GHz, 8GB RAM, and the simulation software is Mathematica 9.0. The secret key generated in this experiment is shown in **Tab. 1**. **Fig. 2** (a) shows a 24-bits colour image with 512*300 pixels and **Fig. 2** (b) shows the encrypted image.

(a) (b)

Fig. 2. The Plaintext Image and the Encrypted Image

Table 1. Secret Key

Key	Value
x_0	0.7
y_0	0.22
α	0.9
H	0.2148
G	96
a	486177307474028755861463367441297832337939857039268554359506144 2
e	63548673
t	8

5. Performance Analysis

5.1 Key space analysis

The key space of an encryption algorithm should be sufficient to resist exhaustive attack. In this paper, the key has 256 bits, therefore, the key space is 2^{256}, where x_0, y_0, α, H, G all have 8 bits, e has 212 bits and t has 4 bits, as shown in **Fig. 3**.

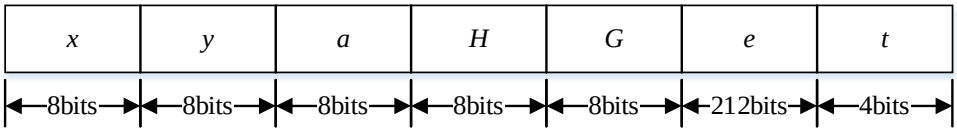


Fig. 3. Key Distribution

5.2 Sensitive analysis

A good encryption algorithm should be sensitive to the change of the secret key by testing the decryption result after one bit of change in the key. There are fewer pixels transferred by Logistic map than by Hénon map, but this finding is not the main reason for being insensitive to the change in the corresponding part key compared with Hénon map. The difference in pixels transferred by Logistic transformation leads to an imparity of pixels that are transformed by Hénon map text; therefore, the change in key corresponding to the Logistic map affects the encryption result to a great extent. However, according to the equations of the initial values in 4.1, in order to make great changes for initial values that will be used in Logistic map, the number of bits should be of reasonable length. According to our experiments, if the key distribution is 32, 32, 32, 32, 24, 100, and 4, the algorithm displays insensitivity to the change of the key; this can be improved significantly by adjusting the key distribution as 8,

8, 8, 8, 8, 212, and 4. Because there are fewer pixels transferred by Logistic map, it can be recognized by changing one bit among the top 40 bits, while it is quite sensitive to the change after the top 40 bits. It is observed that correlation coefficients can be decreased significantly by applying Hénon map at least once. To guarantee the aforementioned effect in a relatively short processing time, we assign 4 bits to the time of Hénon iteration, and set the last bit to 1 by default.

5.3 Time and space complexity analysis

The time cost is one of the metrics to evaluate the algorithm. In [12], if the original image is a non-square image, we should expand it to square first such that the Hénon map can be applied. In this paper, we generated random pixel values in the expanding part since there are no details regarding the expanding operation in [12]. The original image is shown in **Fig. 4**, and the expanded image is shown in **Fig. 5**.

Fig. 4. Original Image

Fig. 5. Expanded Image

The redundant information in the expanded image requires extra space for storage, and the time cost of the Hénon map will be increased. When the worst-case occurs, which means the image expanded $M * (M - 1)$ pixels, where $M = Max(m, n)$, and *m*, *n* are the size of the image. However, the algorithm proposed in this paper does not change the size of the image, hence it does not require extra space to store redundant information and extra operations during iterations. The times consumed by the two algorithms to encrypt the same image are compared in **Fig. 6**, where the parameters in the Hénon map are $a = 45$, $c = 170$.

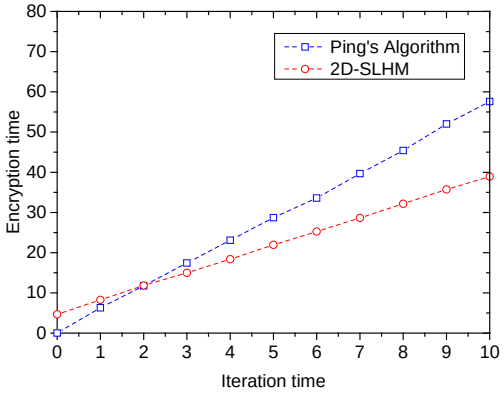


Fig. 6. Comparison Results in Iteration Time

When the Hénon map iterates once, the time cost of our algorithm is higher than that of the algorithm mentioned in [12] due to the complexity. When the Hénon map iterates twice, the time costs of both algorithms are nearly the same. As described in Section 5.1, the algorithm that we proposed requires at least a one-time Hénon map to achieve the scrambling effect, whereas reference [12] reported that it required a minimum of three-time Hénon map. When the iteration time is more than twice, the algorithm in this paper has an advantage in terms of time cost, and this advantage in time increases with respect to the iteration time.

In [11], the proposed algorithm has two rounds of scrambling stage and substitution stage, and the two stages are independent. When only the scrambling stage is considered, each round produces a length of m*n chaotic sequence and subsequently sorts the sequence and makes the corresponding elements of each row into a ring, finally left shifts the number of row elements to achieve the scrambling effect. When the dimension of the image is $N * 1$, there are *N* stationary rings, and the scrambling just sorts the pixels according to the chaotic sequence.

The complexity of time and space comparisons is shown in **Table 2**, Where m, n are the size of the image, and $M = Max(m,\ n)$, $N = m * n - r * r,\ r = \lfloor \sqrt{m * n} \rfloor$.

Table 2. Complexity Comparisons

Algorithm	Time complexity	Space complexity
[11]	$O(n * m * \log m)$	$O(n * m)$
[12]	$O(M * M)$	$O(M * M)$
Proposed	$O(n * \log N)\ or\ O(r * r)$	$O(N)\ or\ O(r * r)$

Use the image from the USC-SIPI 'Aerials' dataset under Mathematica implementation, and crop the image into different sizes 512*512, 256*512, 128*512, 64*512, 32*512, the times consumed by the three algorithms to encrypt the same image are compared in **Fig. 7**.

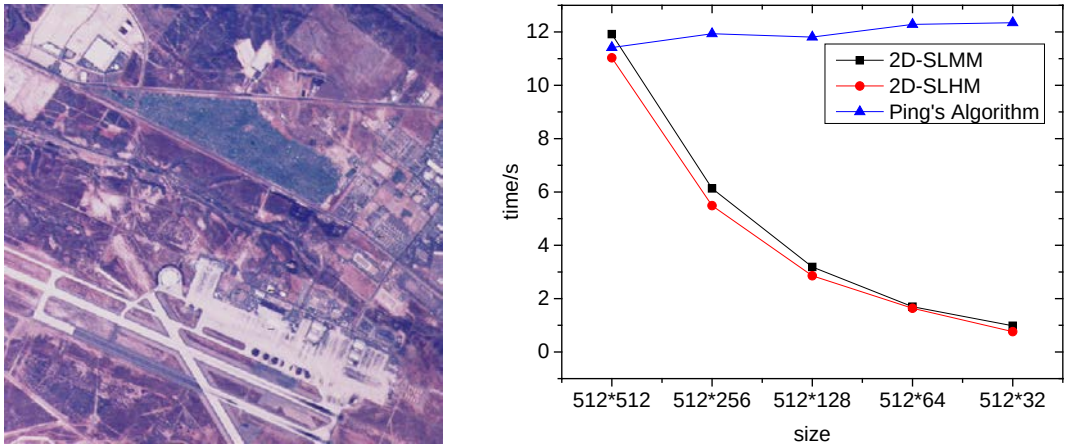


Fig. 7. Comparison Results in Image Scale

From **Fig. 7**, we can see that when the image is square, the time costs of these algorithms are close. When the scale of the image decreases, the time cost of [11] and the proposed algorithm decrease because of fewer computations. When the ratio of length to width is improved, the time consumption of [11] and the proposed algorithm are closer. Because of the expanding stage, the scale changes of image have no effect on the time cost of [12], the expanding computation even increases it. Above all, the results are consistent with the previous analysis. The comparison of time cost applying the three algorithms to 100 arbitrary size images obtained by cropping different images in database CVG-UGR is shown in **Fig. 8**. The time cost of the proposed scrambling algorithm is the lowest of the three algorithms.

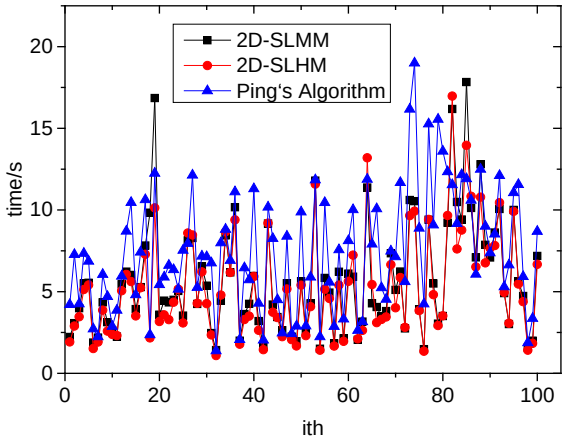


Fig. 8. Time Cost of Different Image Scales

5.4 Correlation coefficient

Correlation coefficient represents the correlation degree of adjacent pixels, it is generally divided into three directions horizontal, vertical and diagonal. The correlation degree of an encrypted image is another metric to evaluate the encryption algorithm. In this paper, we compare the algorithm in [12] with our algorithm by computing the correlation coefficients of all pixels in an encrypted image in three directions. The correlation coefficients are calculated by the following Eqs. (9-12).

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{10}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{11}$$

$$\gamma_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

where x, y represent the values of two adjacent pixels in the image. The original image is processed in the following two steps: (1) it is encrypted separately by the algorithm in [12] and the proposed algorithm in this paper, (2) the horizontal, vertical and diagonal direction correlation coefficients of *R*, *G*, and *B* channels are calculated for all adjacent pixel pairs in the image. **Fig. 9** shows the comparison of [12] and the proposed algorithm for the number of iterations and encryption time.

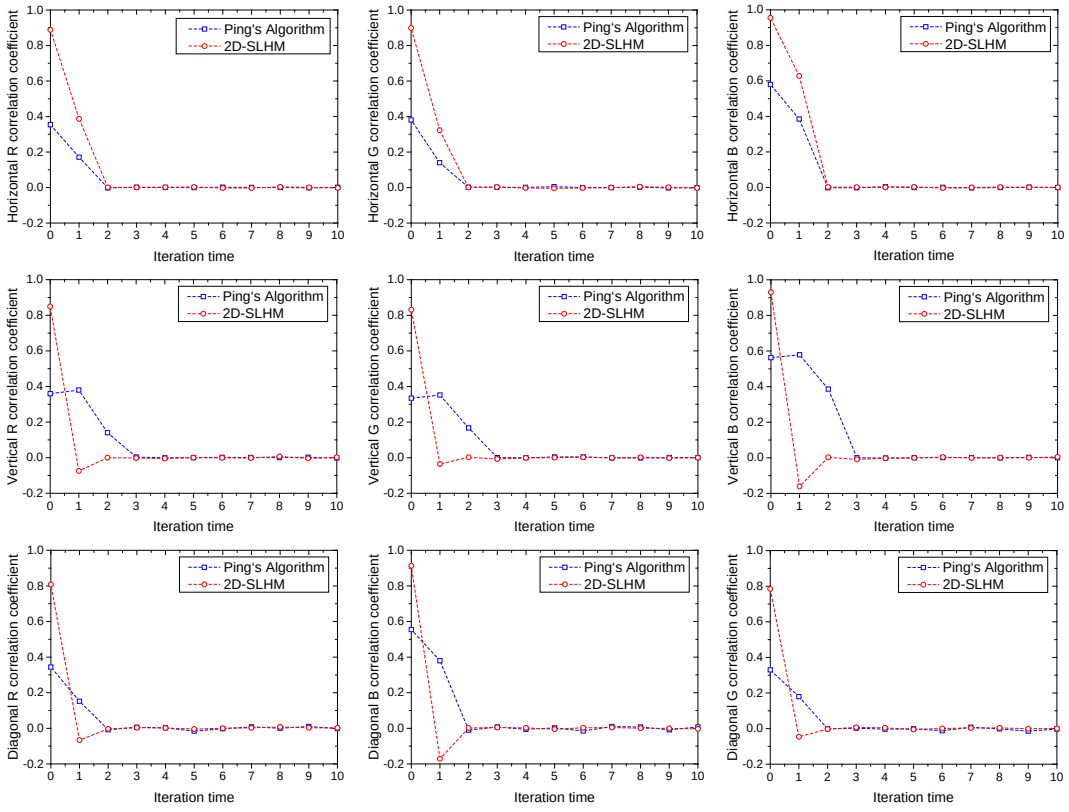
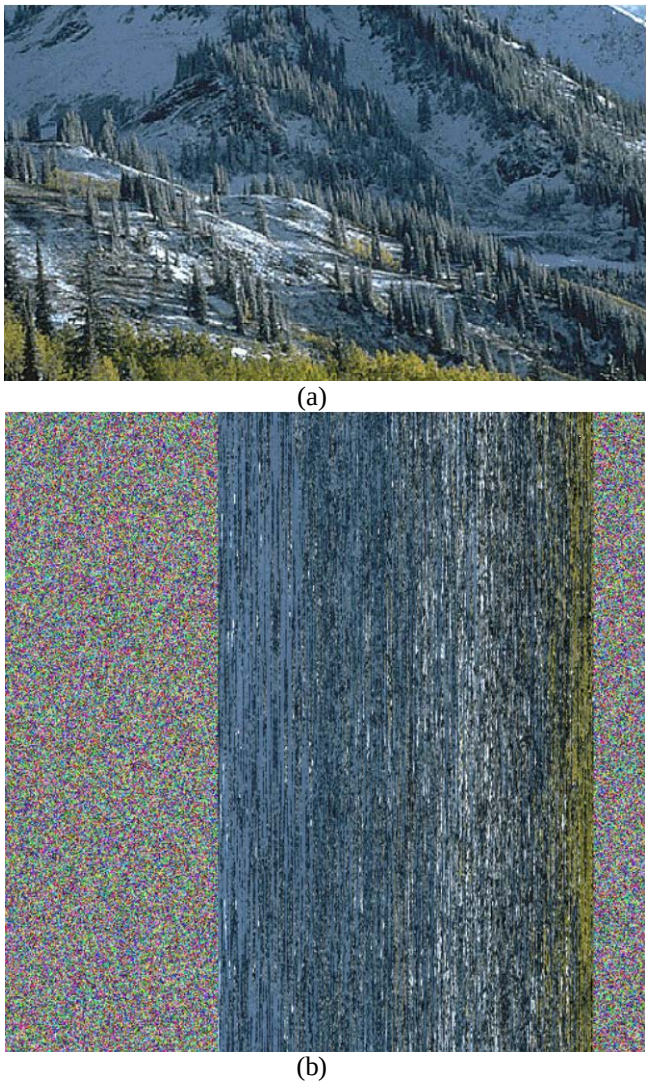


Fig. 9. Correlation Coefficients Comparison

Because we randomly generated the pixel values in the expanded part when encrypting the image by the algorithm in [12], it artificially decreased the correlation coefficients in three directions of the whole image. Therefore, when the iteration time of the Hénon map is zero, the correlation coefficients differ between the two algorithms. It can be observed in **Fig. 9** that,

when the iteration time is 1, the correlation coefficients in three directions decrease significantly by applying our algorithm. In addition, when we increase the number of iteration, the correlation coefficients show slight fluctuations. In comparison, while using the algorithm in [12], the horizontal correlation coefficients decrease significantly after one iteration, and when the iteration time increases, the correlation coefficients also show slight fluctuations. The diagonal correlation coefficient is also decreased, and it shows a steady value after the third iteration. For the vertical direction, its correlation coefficient increases only at the first iteration, decreases at the second iteration, and subsequently remains steady after three iterations. This finding is observed because the original part of the expanded image has regularity when substituted by the Hénon map. The original image and the encrypted image transferred by one-time Hénon map in [12] are shown in **Fig. 10** (a) and (b). The original part of the expanded image still gathered in the middle part of the image that has a high correlation.



(a)

(b)

Fig. 10. Processed by Ping's Algorithm

Apply the [11] and proposed algorithms to 100 arbitrary size images obtained by cropping different images in database CVG-UGR, compute R, G, B channels correlation coefficients

separately. From **Fig. 11**, it can be found that the correlation coefficients are all close to zero, which means that the algorithms have good performance on the scrambling effects.

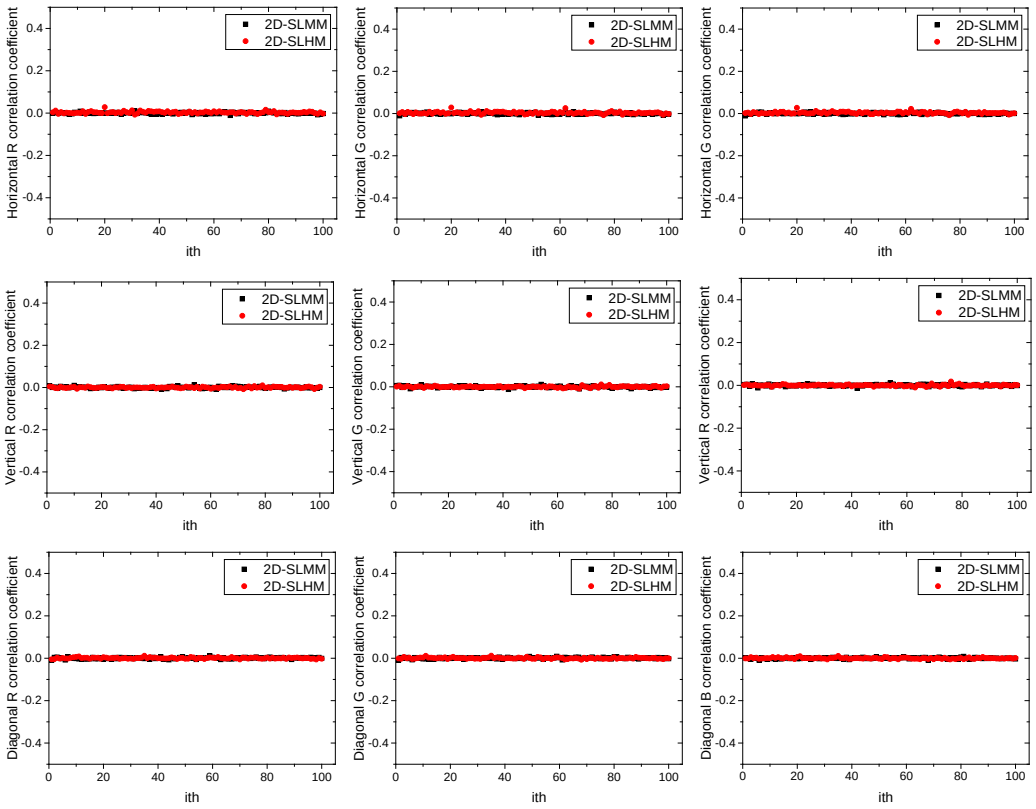


Fig. 11. Correlation Coefficients Comparison

5.5 Chosen-plaintext attack

In [11], the algorithm first generated pairs of sequences by 2D Logistic map, summed up each pair to sort in ascending order, and finally scrambled pixels based on the result of the sorting. The secret key of this algorithm contains the initial statements x, y of the chaotic equations and the controlling parameters α, β, which are generated randomly; such that they are independent of the plain text image. In [12], the algorithm scrambling pixels by Hénon map use the controlling parameters a, c and the iteration time t transformed by randomly generated binary sequence; therefore, they are also independent of the plain text image. In summary, these two algorithms cannot resist the chosen-plaintext attack effectively.

In this paper, the number m of the pixels that require transform by Logistic map is computed according to the size of the original image. Next, the values of all pixels in the plaintext image are summed as the controlling parameter c. Hence, there exists a dual association with the plaintext image. In situations where the image size is unknown, the attacker cannot use the chosen plaintext to attack the Logistic scrambling at the first stage, therefore they cannot use Hénon map to achieve chosen-plaintext attack. In case the attacker is aware of the image size, they may apply Logistic map to scramble at the first stage, but since the pixels scrambled are fewer in this stage and the parameter c is unknown, they still cannot attack using chosen plaintext.

5.6 Robustness to noise

In practice, while transmitting or processing the image, external interference or internal equipment introduces noise to the image. Assume that the algorithm is sensitive to the noise, it cannot accomplish reversing the encrypted image effectively. Therefore, robustness to noise is another metric to evaluate the image scrambling algorithm. To test the algorithm proposed in this paper, Gaussian noise, Salt & Pepper noise and occlusion noise are added to the two different encrypted images Lena and Pepper. In **Fig. 12** (a)(d), (b)(e) and (c)(f) are corresponding the recovered images after adding Gaussian noise of density $\alpha = 0.001, 0.01, 0.1$. In **Fig. 13** (a)(d), (b)(e) and (c)(f) are corresponding the recovered images after adding Salt & Pepper noise of density $\alpha = 0.001, 0.01, 0.1$. In **Fig. 14** (a)(d), (b)(e) and (c)(f) are corresponding the recovered images after adding Occlusion noise of 32*32, 64*64, 128*128. From these figures, we can see that the recovered images can be recognized in all cases.

To evaluate the quality of these recovered images quantitatively, two common similarity measures: the peak signal to noise ratio (PSNR) and the structural similarity index (SSIM) are used in this paper. When the value of PSNR is above 28, the image quality difference is not very significant, and when the above 35 to 40, the naked eye cannot distinguish the difference. The measure of SSIM was developed based on the characteristics of human visual system (HVS), which incorporated the information of structure, luminance and contrast for image quality assessment [20]. When the value of SSIM is close to 1, there is little distortion between the two compared images. **Table. 3** and **Table. 4** presents the PSNR and SSIM measures of each recovered image corresponding to **Fig. 12**, **Fig. 13** and **Fig. 14**. From these tables, we can see that the proposed algorithm demonstrates robustness to noise.

(a) (b) (c)

(d) (e) (f)

Fig. 12. Robustness to Gaussian noise tests

Fig. 13. Robustness to Salt & Pepper noise tests

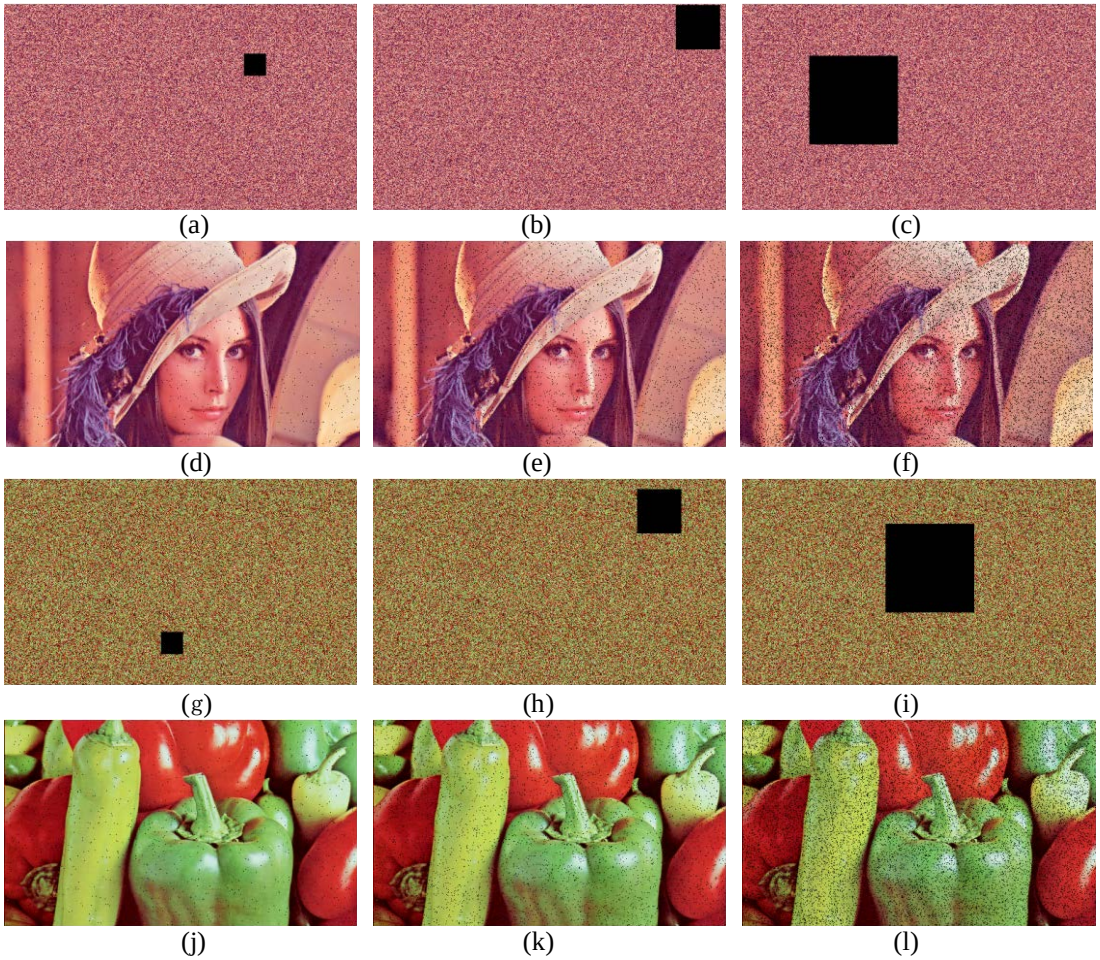


Fig. 14. Robustness to Occlusion noise tests

Table 3. PSNR of Recovered Images

Image	Gaussian			Salt & Pepper			occlusion		
	0.001	**0.01**	**0.1**	**0.001**	**0.01**	**0.1**	**32*32**	**64*64**	**128*128**
Lena	61.9092	44.4420	25.0998	36.6611	26.8376	16.6216	28.5829	22.6307	16.5892
Pepper	62.0048	44.5133	25.1390	36.6130	26.6147	16.6893	29.0761	22.8467	16.7593

Table 4. SSIM of Recovered Images

Image	Gaussian			Salt & Pepper			occlusion		
	0.001	**0.01**	**0.1**	**0.001**	**0.01**	**0.1**	**32*32**	**64*64**	**128*128**
Lena	0.9997	0.9813	0.4664	0.9758	0.7925	0.1972	0.8512	0.5749	0.2552
Pepper	0.9997	0.9814	0.4484	0.9759	0.7824	0.1872	0.8565	0.5745	0.2547

6. Conclusions and Expectations

In this paper, we propose a non-square image scrambling algorithm that can resist chosen-plaintext attack by the combination of chaotic 2D-SLMM and Hénon map. This algorithm can encrypt the digital image without changing the original image size. In the simulation environment of Mathematica 9.0, the prominent cryptographic properties including large key space, execution efficiency and robustness to noise, can be determined by numerical experimental results. The proposed algorithm can resist the chosen-plaintext attack. However, during the process of image scrambling, the serial processing of the pixel is one of the issues that may limit its efficiency. The future research direction is to implement parallel processing of the pixels to improve scrambling efficiency.

Acknowledgments

This paper is partially supported by NSF-China and Guangdong Province Joint Project (Grant No. U1301252), National Natural Science Foundation of China (Grant No. 61272543).

References

[1] W. Ding and D. Qi, “Digital Image Transformation and Information Hiding and Camouflage Techniques,” *Chinese Journal of Computers*, vol. 21, no. 9, pp. 838-843, 1998.
[2] V.I. Arnol′d and A. Avez, *Ergodic problems of classical mechanics*, Benjamin, 1968.
[3] W. Ding, W. Yan, and D. Qi, “Digital image scrambling technology based on Arnold transformation,” *Journal of Computer-Aided Design & Computer Graphics*, vol. 13, pp. 339-341, April, 2001. Article (CrossRef Link)
[4] C. Li, Z. Han and H. Zhang, “The overview on image encryption Technology,” *Journal of Computer Research and Development*, vol. 39, no.10, pp. 1317-1324, 2002.
[5] L. Shao, et al., “The overview on image scrambling,” *Netinfo security*, vol. 4, pp. 22-26, 2009. Article (CrossRef Link)
[6] L. Wan, X. Sun and X. Lin, “Research on Image Encryption Algorithm Based on Fractal Hilbert Curve Mixed Gray Code,” *Computer Engineering and Applications*, vol. 46, no.34, pp. 184-186, 2010. Article (CrossRef Link)
[7] W. Ding, W. Yan, and D. Qi, “Digital Image Scrambling and Digital Watermarking Technology Based on Life Game,” *Journal of North China University of Technology*, vol.1, pp. 1-5, 2000.

[8] D. Qi, "Research and application on matrix transformation in Image Information Hiding," *Journal of North China University of Technology*, vol. 1, pp. 24-28, 1999.
[9] D. Yin, and B. Li, "Using Improved Fibonacci Hash Transform to Increase the Robustness of Meaningful Watermarking Algorithm," *Journal of Wuhan Yejin University of Science & Technology*, vol. 28, no. 3, pp. 266-269, Mar, 2005.
[10] Y. Zhao and X. Sun, "An Algorithm for Scrambling Non - Square Images," *Microcomputer Information*, vol. 27, pp. 99-101+106, 2009. Article (CrossRef Link)
[11] Z. Hua, et al., "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80-94, 2015. Article (CrossRef Link)
[12] P. Ping, et al., "An image scrambling algorithm using discrete Henon map," in *IEEE International Conference on Information and Automation*, 2015. Article (CrossRef Link)
[13] T. Kong and D. Zhang, "A new Arnold inverse transform algorithm," *Journal of Software*, vol. 10, pp. 1558-1564, 2004. Article (CrossRef Link)
[14] C. Qin, et al., "A novel image hashing scheme with perceptual robustness using block truncation coding," *Information Sciences*, vol. 361-362, pp. 84-99, 2016. Article (CrossRef Link)
[15] Q. Mao, C. Chang and H. Wu, "An Image Encryption Scheme Based on Concatenated Torus Automorphisms," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 6, pp. 1492-1511, 2013. Article (CrossRef Link)
[16] X. Wang, L. Teng and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101-1108, April, 2012. Article (CrossRef Link)
[17] C. Li, et al., "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dynamics*, vol. 70, no.4, pp. 2383-2388, 2012. Article (CrossRef Link)
[18] C. Qin, et al., "Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy," *Signal Processing*, vol. 138, pp. 280-293, 2017. Article (CrossRef Link)
[19] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Information Sciences*, vol. 324, pp. 197-207, 2015. Article (CrossRef Link)
[20] C. Qin and X. Zhang, "Effective reversible data hiding in encrypted image with privacy protection for image content," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 154-164, 2015. Article (CrossRef Link)

Siqi Zhou is a graduate student in the College of Computer and Information at Hohai University. She majors in Image Encryption, Cloud Computing, Computer Security.

Feng Xu is a Professor in the College of Computer and Information at Hohai University. His research interests include Cloud Computing, Network Information Security, and Domain Software Engineering.

Ping Ping is an Associate Professor in the College of Computer and Information at Hohai University. Her main research interests are Network Security, Big Data Security, and Information Hiding.

Zaipeng Xie is an Assistant Professor in the College of Computer and Information at Hohai University. His current research interests include embedded systems for cloud computing, and applications of signal processing techniques on experimental measurements of high-energy physical systems.

Xin Lyu is a lecturer in the College of Computer and Information at Hohai University. His research is mainly focused on Cryptography, Network Security and Big Data Privacy Protection.