A Modified Chaos-Based Image Encryption Algorithm

Ming Xu*
Department of Mathematics and Physics, Shijiazhuang Tiedao University, Shijiazhuang, China.

∗ Corresponding author. Tel: +8613400115751; email: 13400115751@126.com

Manuscript submitted April 8, 2015; accepted July 5, 2015.
doi: 10.17706/jsw.10.8.931-938

Abstract: A modified image encryption algorithm based on the Arnold-Chen chaos image encryption algorithm is presented. The original one can't resist chosen-plaintext attack and known-plaintext attack, but the modified algorithm can resist both attacks by simply increasing one key and N horizontal-shifts. The simulation experimental results and security analysis show that the new algorithm has higher security while the encryption speed is as fast as the original one. Moreover, our modified method is transplantable , it can be used to modify other schemes which are easily exposed to differential attack.

Key words: Chaos, differential attack, image encryption, transplantable.

1. Introduction

An image encryption scheme was proposed in [1] which used Arnold's cat map to shuffle the pixels and Chen's chaotic system to change the gray levels of the pixels. The scheme can't resist chosen-plaintext attack and known-plaintext attack, Cokal and Solak gave a complete break to it in [2]. Based on the scheme in [1], we propose a modified scheme which can resist both attacks by simply increasing one key and N horizontal-shifts.

In fact, many image encryption algorithms[1], [3]-[5] have weak ability of resisting differential attack [2], [6]-[8]. The conventional improved solution is increasing the rounds of encryption, but it will undoubtedly increase the running time and computational complexity. Compared with the conventional improved solution, our solution is more efficient. Moreover, it is transplantable, it can be also used to modify other encryption algorithms which easily be attacked by differential attack.

The outline of this paper is as follows: In the next section we describe the original encryption algorithm and corresponding attack scheme briefly, meanwhile analyze the reason why the original algorithm easily be attacked. In Section 3, we propose a modified scheme which can resist the chosen-plaintext attack and known-plaintext attack. In Section 4, we give comparison of the two schemes by simulation experiments. Finally, we give concluding remarks.

2. Description of the Original Encryption Algorithm and Corresponding Attack Scheme

2.1. Arnold Cat Map

Assume that we have an *N*×*N* image *P* with the pixel coordinates $I=\{(x,y)\mid x,y=0,1,2,\ldots,N-1\}$, Arnold cat map is given as

where *p*, *q* are positive integers and x',y' are the coordinate values of the shuffled pixel. After iterating this map *n* times, we have

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A^n\begin{bmatrix} x \\ y \end{bmatrix} = M\begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2}$$

where $M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = A^n \bmod N$

The shuffled image *S* is related to the original image *P* as

$$S(x', y') = P(x, y). \quad 0 \le x, y \le N-1 \tag{3}$$

2.2. Chen's Chaotic System

Chen's chaotic system is a set of differential equations given as

$$\begin{aligned} \dot{x} &= c(y-x), \\ \dot{y} &= (c-a)x - xz + cy, \\ \dot{z} &= xy - bz, \end{aligned} \tag{4}$$

where *a*, *b* and *c* are parameters of the system. Chen's system is chaotic when the parameters have values: *a*=35, *b*=3 and $c \in [20, 28.4]$.

2.3. Original Image Cryptosystem

1) The secret keys of original algorithm are parameters *p*, *q*, *n* of Arnold cat map and initial values x_0, y_0, z_0 of Chen's chaotic system, the encryption steps are as follows:
2) The image firstly be shuffled by Arnold cat map as (2), then the shuffled image is converted into a sequence *S*;
3) A pseudo random key sequence *K* is produced by Chen's chaotic system (4) subsequently. Using *K* to do bitwise XOR operation with *S*, the encrypted sequence *C* can be produced as:

$$C = S \oplus K \tag{5}$$

4) By reshaping the sequence *C* into an *N*×*N* image, the final ciphertext image is obtained.

2.4. Corresponding Attack Scheme

1) Chosen-plaintext attack: the attacker chooses an image P_1 that consists of *N*×*N* zero-valued pixels, and obtains the corresponding ciphertext image C_1. The shuffling process does not change the image because P_1 is identically 0. Hence, the shuffled image S_1 is equal to image P_1. Using this fact and encryption formula (5), the attacker can easily find that the cipher-image *C* is exactly equal to the key *K* as:

$$C = S \oplus K = P_1 \oplus K = 0 \oplus K = K \tag{6}$$

After obtaining *K*, the attacker can then compute the scrambling matrix *M* as in [2]. However, in our modified algorithm, the attacker can't obtain *K* except using brute-force attack, hence he can't extract *M* either, then the chosen-plaintext attack is invalid for our algorithm.

2) Known-plaintext attack: Assume that the attacker knows two plaintext–ciphertext image pairs (P_1, C_1) and (P_2, C_2). Define the differences as $\triangle P = P_1 \oplus P_2$ and $\triangle C = C_1 \oplus C_2$. The known-plaintext attack is based on the following formula:

$$\triangle C = S_1 \oplus K \oplus S_2 \oplus K = S_1 \oplus S_2 = \triangle S \tag{7}$$

Using (7), the attacker can calculate $\triangle S$ from $\triangle C$. Going from $\triangle P$ to$\triangle S$, there is only shuffling by the Arnold cat map, a method to reveal the parameters of this map is given in [2], thus the encryption scheme is successfully broken. However, in our modified algorithm, (7) is not tenable any more, so the attacker can't carry on the following attack, the known-plaintext attack is also invalid for our modified algorithm.

From the description above, we can see the reason why the original scheme easily be attacked: the substitution and permutation of pixels are independent of the plaintext image. Based on this consideration, we put forward our modified algorithm.

3. Modified Arnold-Chen Chaos Image Cryptosystem

The secret keys of the modified algorithm are the parameters p, q, n of Arnold cat map , the initial values x_0, y_0, z_0 of Chen's chaotic system and an initial key u_0.

3.1. Encryption Algorithm

The encryption steps are as follows:

Shuffle the image P using Arnold cat map as (2) and obtain the shuffled image S.

1) By scanning the shuffled image S row-by-row, rearrange its pixels to obtain the sequence S= $\{s_{11}, s_{12}, ..., s_{1N}; s_{21}, s_{22}, ..., s_{2N}; ...; s_{N1}, s_{N2}, ..., s_{NN};\}$

where s_{ij} is the pixel of S located in the ith row and jth column.

2) Using Runge-Kutta step size 0.001, iterate Chen's chaotic system N_0=(N×N)/3 times and obtain the real values x_i, y_i, z_i, $1 \le i \le N_0$.

3) Compute the key sequence $K = \{k_1, k_2, ..., k_{N\times N}\}$ as

$$\begin{aligned} k_{3(i-1)+1} &= \left|x_i - \lfloor x_i \rfloor\right| \times 10^{14} \bmod 256, \\ k_{3(i-1)+2} &= \left|y_i - \lfloor y_i \rfloor\right| \times 10^{14} \bmod 256, \\ k_{3(i-1)+3} &= \left|z_i - \lfloor z_i \rfloor\right| \times 10^{14} \bmod 256, \end{aligned} \tag{8}$$

where $\lfloor x \rfloor$ denotes the largest integer not larger than x.

4) Firstly, assign 0 to i, and convert the initial key u_0 to unsigned integer u in the range of 0 to 255, subsequently assign u to variation d (d denotes the step length of horizontal-shift), then for each row of the image S(from i=0 to i=N—1), repeat the following operations:

a) Compute a new sequence $C' = \{c_0{}', c_1{}', ..., c_{N-1}{}'\}$ as

$$c_j{}' = s_{ij} \oplus k_{i\times N+j+1} \qquad 0 \le j \le N-1 \tag{9}$$

where $\oplus$ represents bitwise exclusive OR operation, i denotes the order of current row, j changes from 0 to N—1;

b) Construct the sequence $S_1 = \{u, c_0{}', c_1{}', ..., c_{N-1}{}'\}$, then do horizontal shift on S_1 by d pixels, a new sequence $S_2 = \{s_0{}', s_1{}', ..., s_N{}'\}$ is obtained.

c) Get the ith row of final ciphertext image C as

$$c_{ij} = s_i{}' \qquad j = 0, 1, ..., N-1,$$

Meanwhile assign the last pixel $s_N{}'$ of S_2 to variation u, assign $c_{i(N-1)} \oplus k_{(i+1)N}$ to d;

d) $i = i + 1$. If *i*<*N*, go back to (i); if *i*=*N*, jump out of the loop.

At the end of (5), we can get the final ciphertext image *C* and a ciphertext *u*;

3.2. Decryption Algorithm

The decryption steps are as follows:

1) Using Runge-Kutta step size 0.001, iterate Chen's chaotic system N_0=(*N*×*N*)/3 times and obtain the real values x_i, y_i, z_i, 1≤*i*≤N_0.
2) Compute the key sequence $K = \{k_1, k_2, ..., k_{N\times N}\}$ as (8).
3) Firstly, assign *N*—1 to *i*, then for each row of the ciphertext image *C*(from *i*=*N*—1 to *i*=1), repeat the following operations:

a) Compute *d*= $c_{i-1,N-1} \oplus k_{i\times N}$, where $c_{i-1,N-1}$ denotes the pixel of *C* located at ($i-1$)th row and ($N-1$)th column. Construct the sequence $S_2 = \{c_{i0}, c_{i1}, ..., c_{i(N-1)}, u\}$, where c_{ij} $(j = 0, ..., N-1)$ are the *N* pixels in the current row(*i*th row). Do horizontal shift on S_2 by *d* pixels in the direction opposite to encryption's, then we can obtain a new sequence $S_1 = \{s_0', s_1', ..., s_N'\}$;

b) Assign s_0' to *u*, meanwhile obtain the *i*th row of image *S* as

$$s_{ij} = s_{j+1}' \oplus k_{i\times N+j+1} \qquad 0 \le j \le N-1 \tag{10}$$

c) $i = i - 1$. If *i*>=1, go back to (i); if *i*=0, jump out of the loop and go to (4).

4) Construct the sequence $S_2 = \{c_{00}, c_{01}, ..., c_{0(N-1)}, u\}$, c_{0j} $(j = 0, 1, ..., N-1)$ are the *N* pixels in the first row of cipher image *C*, do horizontal shift on S_2 by u_0 pixels in the direction opposite to encryption's(u_0 is the initial key), we can obtain a new sequence $S_1 = \{s_0', s_1', ..., s_N'\}$, then the first row of image *S* is computed as

$$s_{0j} = s_{j+1}' \oplus k_{j+1} \qquad 0 \le j \le N-1 \tag{11}$$

5) Shuffle the image *S* using anti-Arnold cat map, then the plaintext image *P* is recovered.

4. Comparison of the Original and Modified Cryptosystems

This section provides the simulation results of original algorithm and modified algorithm. In those simulation experiments, we set the secret keys of both algorithms as: the parameters of Arnold cat map are *p*=1, *q*=1, *n*=5; the initial values of Chen's chaotic system are x_0=—10.058, y_0=0.368, z_0=37.368, the parameter *c* is 28; besides, the initial key u_0 of modified algorithm is 112.

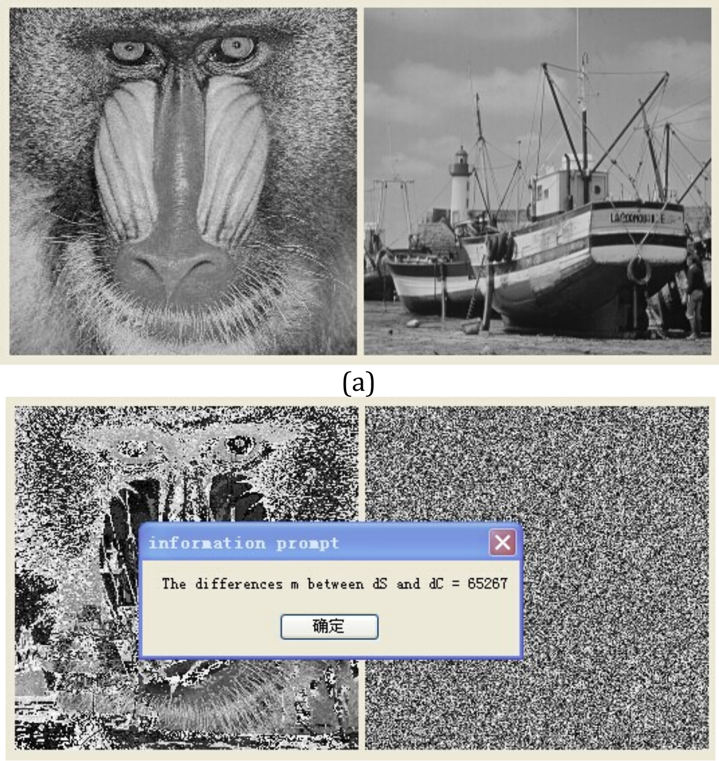
4.1. The Ability of Resisting Differential Attack

From Section 2, we know that the original algorithm can't resist both chosen-plaintext attack and known-plaint attack. Now we discuss the modified one.

For the image P_1 mentioned above which consists of *N*×*N* zero-valued pixels, the shuffling process does not change the image yet, but the formula (5) is not satisfied in the modified algorithm, so we can't compute *K* from (6) as in the original algorithm. In fact, the ciphertext image of P_1 is not *K* but a shuffled *K*. Therefore the modified algorithm can resist chosen-plaintext attack.

The known-plaintext attack to the original algorithm is actually differential attack. The reason for that the differential attack is feasible in original algorithm is (7). Using (7), the attacker can calculate △*S*(=△C), going from △*P* to △*S*, there is only shuffling by the Arnold cat map. But in our modified algorithm, △

S≠△C, so the differential attack cannot be continued. The simulation results are shown in Fig. 1.



The differences m between dS and dC = 65267

(a)

(b)

Fig. 1. (a) Plaintext images P_1 and P_2. (b) Difference images △P and △C.

From the simulation experiments, we find that the number of different pixels between △S and △C is 65267, we can't obtain any information of △S from △C.

Next, we will compare the two algorithms from the following respects.

4.2. Histogram Analysis

An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated the histograms of the encrypted images in both algorithms, the results of histogram analysis are shown in Fig. 2.

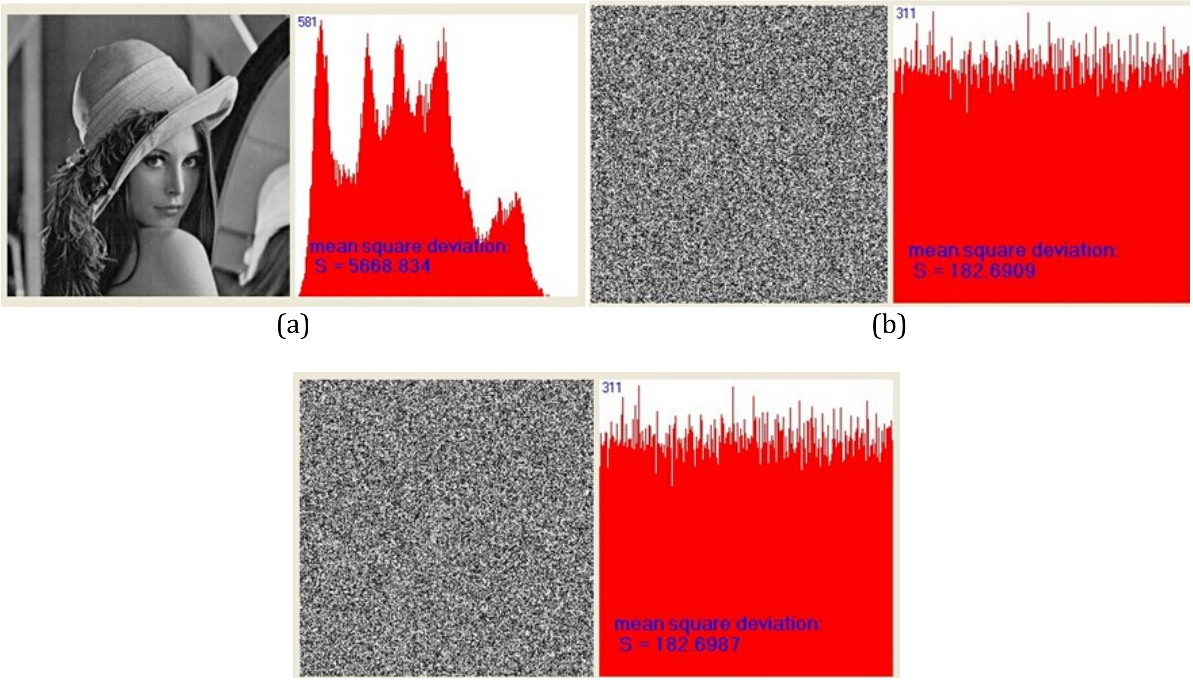
It is clear from Fig. 2 that there is little difference between the histograms of encrypted images in the two algorithms(because we do only shuffling operations on the basis of original algorithm). Moreover, the histograms of two encrypted images are fairly uniform and significantly different from the histogram of plaintext image, so it does not provide any clue to the statistical attack.

4.3. Information Entropy Analysis

For testing the robustness of encryption algorithm, the concept of entropy is also used. The higher the entropy of encrypted image is, the better the security is. The information entropy of encrypted images in original and modified algorithms are both 7.996925, which is very near to the maximum of entropy value 8. It indicates that in encrypted image all the pixels occur with almost equal probability , thus the two algorithms can successfully resist entropy attack.

4.4. Correlation Coefficient Analysis

In addition to the histogram analysis and entropy analysis, we have also analyzed the correlation between two adjacent pixels in the images. The results of correlation coefficient analysis are shown in Fig. 3.

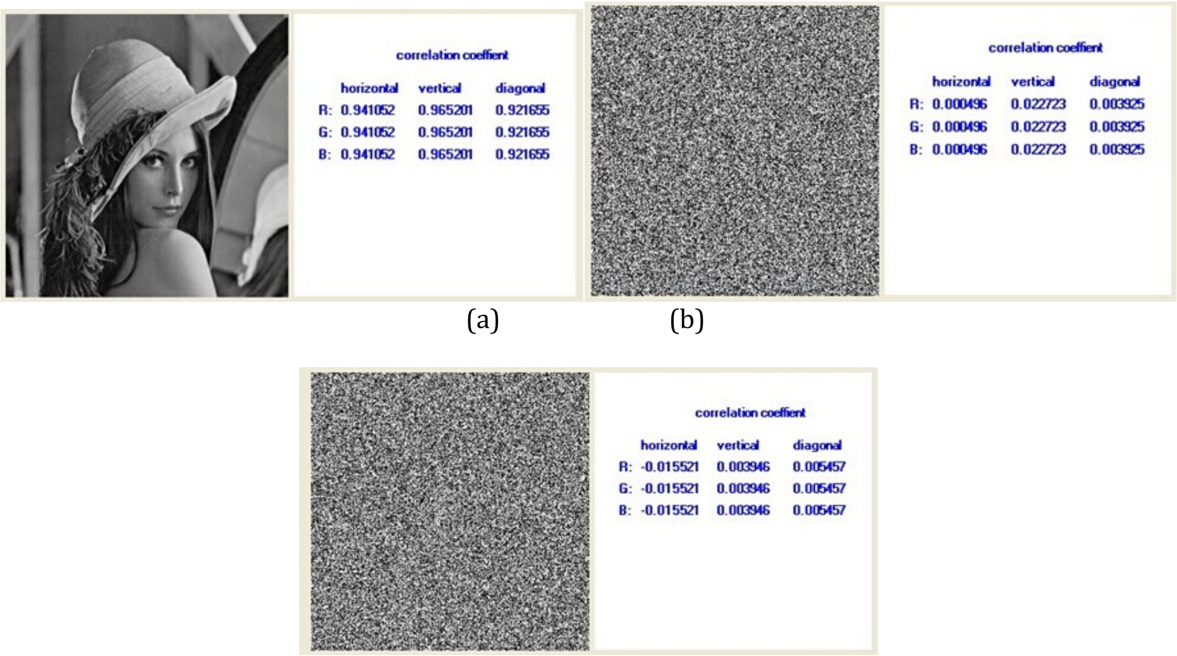


(a)

(b)

(c)

Fig. 2. (a) Plaintext *P* and its histogram. (b) Cipher-image of *P* in original algorithm and its histogram. (c) Cipher-image of *P* in modified algorithm and its histogram.


correlation coeffient

	horizontal	vertical	diagonal
R:	0.941052	0.965201	0.921655
G:	0.941052	0.965201	0.921655
B:	0.941052	0.965201	0.921655

correlation coeffient

	horizontal	vertical	diagonal
R:	0.000496	0.022723	0.003925
G:	0.000496	0.022723	0.003925
B:	0.000496	0.022723	0.003925

(a) (b)

correlation coeffient

	horizontal	vertical	diagonal
R:	-0.015521	0.003946	0.005457
G:	-0.015521	0.003946	0.005457
B:	-0.015521	0.003946	0.005457

(c)

Fig. 3. (a) Plaintext image and its correlation coefficient. (b) Cipher-image in original algorithm and its correlation coefficient. (c) Cipher-image in modified algorithm and its correlation coefficient.

From Fig. 3 we can see that the horizontal and diagonal correlation coefficients in modified algorithm are a little bigger than that in original algorithm, the vertical correlation coefficient is a little smaller than that in original algorithm, but they are all much smaller than the plaintext image's. It is easy to understand, because in the modified algorithm, we increase the correlation of pixels to resist differential attack.

4.5. Differential Analysis

The aim of this analysis is to determine the sensitivity of encryption algorithm to slightest changes. Two criteria NPCR and UACI are used to test the sensitiveness. Number of pixels change rate (NPCR) is defined as the percentage of different pixel numbers between two encrypted images, whose plaint-images have only one pixel difference. Unified average changing intensity (UACI) is defined as the average intensity of difference between two cipher images, corresponding to plaint- images that have only one pixel difference. The high values of these two parameters indicate that small change in plaint-image creates significant change in the ciphered images. In the simulation experiment we choose image "Lena" as the plaintext image, the values of NPCR and UACI in the original algorithm are 0.0015% and 2.99E－05% respectively, so it is easily attacked by differential attack. But the two values in modified algorithm are 99.62% and 33.52% respectively, hence the modified algorithm is highly resistive against differential attack.

4.6. Encryption Speed Analysis

We have compared the two algorithms in image encryption speed. An 256×256 image "Lena" is encrypted, the running time of encryption process in original algorithm is 60.48 milliseconds, while the running time in modified algorithm is 80.26 milliseconds. The results show that the encryption speed in the two algorithms are very nearly the same.

4.7. The Comparison of Our Improvement Solution with the Conventional One

One can also utilize the conventional improvement solution to raise the values of NPCR and UACI, i.e. increasing the rounds of encryption. The simulation results show that if one wants the NPCR to achieve 99.6257%, he needs 3 rounds of encryption, approximately 170.36 milliseconds. So it is easy to see that our improvement solution is more efficient.

5. Conclusions

In this paper we propose a modified image encryption scheme based on the Arnold-Chen chaos image encryption scheme. The original one can't resist chosen-plaintext attack and known-plaintext attack, but our algorithm can resist both attacks by simply increasing one key and *N* horizontal-shifts. The experimental results show that the cipher in our algorithm has good randomness, can resist statistical analysis and difference analysis. Moreover, compared with the original scheme, the running time is not obviously increased. Thus the scheme proposed in this paper has higher security and faster encryption speed. Especially, our improvement method is portable , it can be also used to modify other image encryption schemes that are easily exposed to differential attack.

Acknowledgement

The first author thanks Hebei Province Natural Science Foundation of China through the Grant No. A2014210104.

References

[1] Guan, Z. H., Huang, F. J., & Guan, W. J. (2005). A chaos-based image encryption algorithm. *Physics Letters A, 346*, 153-157.

[2] Cokal, C, & Solak, E. (2009). Cryptanalysis of a chaos-based image encryption algorithm. *Physics Letters A*, *373*, 1357-1360.

[3] Fridrich, J. (1998). Symmetric ciphers based on two dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, *8*,1259-1284.

[4] Tong, X. J., & Cui, M. (2008). Image encryption with compound chaotic sequence cipher shifting dynamically. *Image and Vision Computing, 26*, 843-850.

[5] Liu, L., Zhang, Q.,＆Wei, X. (2012). A RGB image encryption algorithm based on DNA encoding and

chaos map. *Computers and Electrical Engineering, 38*, 1240–1248.

[6] Solak, E., Cokal, C., & Yildiz, O. T. (2010). Cryptanalysis of Fridrich's chaotic image encryption. *International Journal of Bifurcation and Chaos, 20*, 1405-1413.

[7] Li, C. Q., Li, S. J., & Chen, G. R. (2009). Cryptanalysis of an image encrypion scheme based on a compound chaotic sequence. *Image and Vision Computing, 27*, 1035-1039.

[8] Ozkaynak, F., Ozer, A., & Yavuz, S. (2013). Security analysis of an image encryption algorithm based on chaos and DNA encoding. *Proceedings of the International Conference on Signal Processing and Multimedia Applications.*

[9] Period of the discrete Arnold cat map and general cat map. Retrieved 2012, from http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.

Ming Xu was born in China, in 1981. She received her master in applied mathematics from Northeastern University, Shen Yang, China. She received her PhD degree in 2006. Her main research fields is cryptography.