An Improved Image Encryption Algorithm based on Chaotic System

Shubo Liu[1,2], Jing Sun[1,2], Zhengquan Xu[1]
1 State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan, Hubei, China, 430079
2 Computer School of Wuhan University, Wuhan, Hubei, China, 430079
E-mail:liu.shubo@163.com, sunjing528@163.com, xuzq@whu.edu.cn

Abstract—**The security of stream cipher, which is known as one of the main cipher techniques, is dependents completely on the quality of generated pseudo-stochastic sequences. Chaotic systems can produce the pseudo-random sequences with good randomness , therefore, these systems are suitable to the stream cipher. In this paper, a new encryption algorithm is proposed by analyzing the principle of the chaos encryption algorithm based on logistic map. Moreover, the security and performance of the proposed algorithm is also estimated. The experimental results based on coupled chaotic maps approve the effectiveness of the proposed method, and the coupled chaotic maps shows advantages of large key space and high-level security. The ciphertext generated by this method is the same size as the plaintext and is suitable for practical use in the secure transmission of confidential information over the Internet.**

Index Terms—**Logistic map; Stream cipher; Image encryption;**

I. INTRODUCTION

Chaos theory has been established since 1970s by many different research areas, such as physics, mathematics, engineering, and biology, etc. [1]. Since 1990s, many researchers have noticed that there exists the close relationship between chaos and cryptography [2, 3]. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, have granted chaotic dynamics as a promising alternative for the conventional cryptographic algorithms. Chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps which are deterministic but simple. Therefore, it can provide a fast and secure means for data protection, which is crucial for multimedia data transmission over fast communication channels, such as the broadband internet communication.

Chaos seems to be a good candidate due to its ergodicity and complex dynamics. However, chaotic systems are usually assumed to work in the real number domain, and hence the speed is limited for actual implementation. On the other hand, its randomness nature will be deteriorated when a finite precision with fixed-point arithmetic is used. Moreover, some severe problems have been observed，such as short cycle length, non-ideal distribution and high-correlation[4].

In this paper, the protection of images is particularly in interested, while most conventional ciphers, such as DES, IDEA, and AES [5, 6], are not suitable for image encryption in real time，because their speed is slow due to a large data volume and strong correlation among image pixels. In recent years, a number of chaos-based cryptographic schemes have been proposed [3, 25, 7-22], where most of them are based on block transform utilizing the chaotic map. To enhance security, the dimension of these maps has been extended from one to three. Among them, chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power etc.

The characteristics of the chaotic maps have attracted the attention of cryptographers to develop new encryption algorithms with higher security and speed. There are some chaos-based image cryptosystems with their own structure. For example, Pareek et al. [13] proposed an image encryption scheme which utilizes two chaotic logistic maps and an external key of 80-bit. The initial conditions for both logistic maps were derived using the external secret key. The first logistic map was used to generate numbers in the range between 1 and 24 and the initial condition of the second logistic map was modified by the numbers generated by the first logistic map. The authors showed that by modifying the initial condition of the second logistic map in this way, its dynamics became more random. Kwok et al. [15] proposed a fast chaos-based image cryptosystem with the architecture of a stream cipher. In particular, the plain-image pixels are masked by a pseudo-random keystream generated by a cascade of the skewed tent map and a high-dimensional cat map. Behnia et al. [20] proposed a novel algorithm for image encryption based on mixture of chaotic maps, using one dimensional chaotic map and their coupling to obtain high level security [23,24].

It can be noticed that most of the image encryption designs are in the form of block cipher, which is usually considered faster than its counterpart, stream cipher, although stream cipher may provide better security under

Project number：No. 2006CB303104 and No. 40871200.
Corresponding author: Zhengquan Xu.

the concept of perfect security. In this paper, a novel image encryption algorithm based on logistic map is proposed, and it is demonstrated that a well-designed chaos-based stream cipher can be a good candidate and may even outperform the block cipher, on speed and security. In it, the keystream generator is based on coupled chaotic logistic maps that one logistic chaotic system generates the satisfied random number to update the parameter of the other. The chaotic binary sequence is perturbed by XOR operation on its own three parts. The encryption step proposed in the algorithm consists of a simple bitwise XOR operation of the plaintext binary sequence with the keystream binary sequence to produce the ciphertext binary sequence. Then, a detailed statistical analysis on the proposed encryption scheme is given. The experimental results based on coupled chaotic maps approve the effectiveness of the proposed method, and the coupled chaotic maps shows advantages of large key space and high-level security. Having a high throughput, the proposed system is ready to be applied in fast real time encryption applications.

The organization of this paper is as follow. In Section 2, the design of the proposed chaos-based image encryption scheme is discussed in detail, while the design of a new chaos-based pseudo-random generator is given. The performances and the cryptanalysis of the proposed image encryption scheme are studied in Section 3. Finally, conclusion remarks are drawn in Section 4.

II. THE PROPOSED IMAGE ENCRYPTION ALGORITHM

A. Chaos-Based Pseudo-Random Keystream Generator

In this paper, the major part of the design is a newly proposed chaos-based pseudo-random keystream generator (PRKG) based on a couple of chaotic systems. The structure of the PRKG system is presented in Fig. 1. The two logistic chaotic systems use the same principle with different initial values. In our design, the first logistic chaotic system generates the random numbers to update the parameters of the second, while some conditions are satisfied. The generator system is proposed in the following.

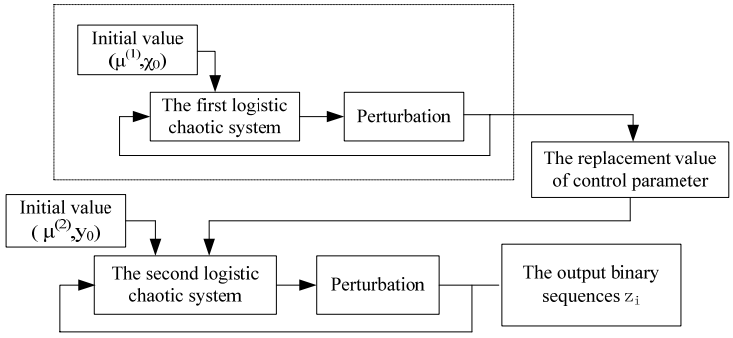

Figure 1. The key stream generator system.

(a) Quantification Method

Generating a pseudorandom binary sequence from the orbit of the logistic map

$$x_{n+1} = \mu x_n(1-x_n) \quad (1)$$

For $\chi_n \in (0,1)$ and $\mu \in (3.569945,4]$, μ and χ_n are the system control parameter and initial condition. Depending on the value of μ, the dynamics of the system can change dramatically. The choice of μ in the equation above guarantees the system is in chaotic state and output chaotic sequences $\{\chi_n\}$ have perfect randomness [25, 26].

A simple way for turning a real number χ_n to a discrete bits symbol X_n is presented by Eq. (2). Change the decimal part of the real into the binary sequences, and then extract some bits form it, so X_n is $\{b_{n1},b_{n2},b_{n3},\ldots b_{nL}\}$. We also can turn the binary representation X_n to its corresponding real representation χ_n by the reverse operation of Eq. (2).

$$\begin{aligned} x_n &= 0.b_{n1}b_{n2}...b_{nL} \\ &= 2^{-1}b_{n1} + 2^{-2}b_{n2} + ... + 2^{-L}b_{nL} \end{aligned} \quad (2)$$

(b) Keystream Generator

The new generator system adopting two logistic maps is proposed for the generation of pseudorandom binary sequences. This algorithm consists of two logistic maps:

$$\begin{aligned} x_{n+1} &= \mu^{(1)} x_n(1-x_n) \\ y_{n+1} &= \mu^{(2)} y_n(1-y_n), n = 0, 1, 2... \end{aligned} \quad (3)$$

for $\chi_n \in (0,1)$ and $\mu \in (3.569945,4]$, evolve successive states from the first logistic map by $\chi_{n+1}=\mu^{(1)}\chi_n(1-\chi_n)$, and obtain the real number χ_{n+1} , turn the real number χ_{n+1} to its binary representation X_{n+1} by Eq. (2), suppose that L=45, thus X_{n+1} is $\{b_1,b_2,b_3,\ldots b_{45}\}$. By defining three variables whose binary representation is $X_l=b_1\ldots b_{15}$, $X_m=b_{16}\ldots b_{30}$, $X_h=b_{31}\ldots b_{45}$, respectively, the following equations are obtained.

$$X_{n+1}' = X_l \oplus X_m \oplus X_h \quad (4)$$

Suppose that X_{n+1}' is $\{p_1\ldots p_{15}\}$ after XOR operation, we turn the X_{n+1}' to its real representation χ_{n+1}' by Eq. (5). χ_{n+1}' is extended till tens to meet the condition: $\chi_{i+1}'' \in (3.569945,4]$, so that the value can make the sequences into chaos. Then, judge whether the condition: $3.569945 < \chi_{i+1}'' \le 4$ and $c \ge 100$ is valid or not, in it, variable c is the iterative times since last update of $\mu^{(2)}$. If valid, χ_{i+1}'' is used to update the parameter $\mu^{(2)}$ of the second logistic map system. In the iterative process, χ_{n+1}' is always to update the value of previous iteration χ_n.

$$x_{n+1}' = 2^{-1}p_1 + 2^{-2}p_2 + ... + 2^{-15}p_{15} \quad (5)$$

$$x_{n+1}'' = x_{n+1}' \times 10 \quad (6)$$

$$\mu^{(2)} = x_{i+1}'' \quad (3.569945 < x_{i+1}'' \le 4 \cap c \ge 100) \quad (7)$$

The second logistic map does the same operations except for Eq. (6) and Eq. (7). Evolve successive states from the second logistic map by $y_{n+1}=\mu^{(2)}y_n(1-y_n)$, and obtain the real number y_{n+1} , turn the real number y_{n+1} to its binary representation Y_{n+1} by Eq. (2), then we can get the value Y_{n+1}' by XOR operation expressed in Eq. (4), Y_{n+1}' is the output binary sequences z_i, meanwhile, turn the Y_{n+1}' to its real representation y_{n+1}', and y_{n+1}' is to update the value of previous iteration y_n.

Briefly, the algorithm can be expressed as follows:

1. $x_{i+1} = \mu^{(1)} x_i (1 - x_i)$
   $y_{i+1} = \mu^{(2)} y_i (1 - y_i), i = 0, 1, 2...$
2. $x_{i+1} \to X_{i+1}, \quad y_{i+1} \to Y_{i+1}$
3. $X_{i+1}' = X_l \oplus X_m \oplus X_h$
   $Y_{i+1}' = Y_l \oplus Y_m \oplus Y_h$
4. $X_{n+1}' \to x_{n+1}', \quad Y_{n+1}' \to y_{n+1}'$
5. $x_{i+1}'' = x_{i+1}' \times 10$
   $\mu^{(2)} = x_{i+1}'' \quad (3.569945 < x_{i+1}'' \le 4 \cap c \ge 100)$
6. $x_i = x_{i+1}', y_i = y_{i+1}'$
7. $z_i = Y_{n+1}'$

B. Design of Encryption and Decryption Scheme

In this section, a chaos-based image encryption system, in the framework of stream cipher architecture, is proposed. The chaos-based image encryption scheme is shown in Fig. 2. An image is firstly converted to a binary data stream. By masking these data with a random keystream generated by the chaos-based PRKG explained before, the corresponding encrypted image is formed. The details of encryption and decryption scheme are to be discussed in the following Fig. 3. As demonstrated in our simulation, this approach is light-weighted and performed well both in security and speed.

As explained in Section 2.1, the PRKG is governed by a couple of logistic maps, which is depended on the values of ($\mu^{(1)}$,χ_0, $\mu^{(2)}$,y_0). These values are secreted, and be used as the cipher key. Through iterations, the first logistic map generates a hash value, which is highly dependent on the input (i.e. the user key), is obtained and used to determine the system parameters of the second logistic map. Then, the hash value will be enlarged till ten times. If the new obtained hash value is in the finite area $3.569945<\mu\le4$, meanwhile, $c\ge100$, the system parameter of the second logistic map will be updated by it. The second logistic map also generates a hash value, which is highly dependent on the input (i.e. the user key) and the first logistic map, is obtained and used to masking the data stream of the plain image. Because in the plain image, the gray-scale values is in the range [0, 255], we implement the operation by Eq. (8).

$$z_i' = z_i \mod 256 \quad (8)$$

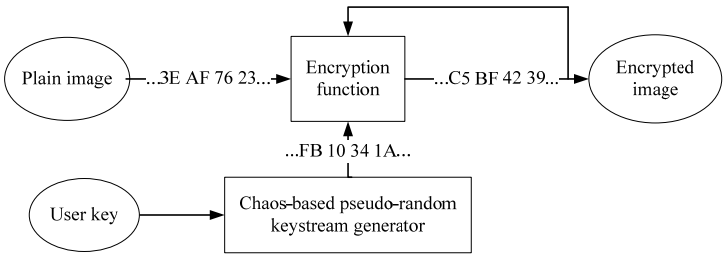

Figure 2. Chaos-based image encryption scheme.

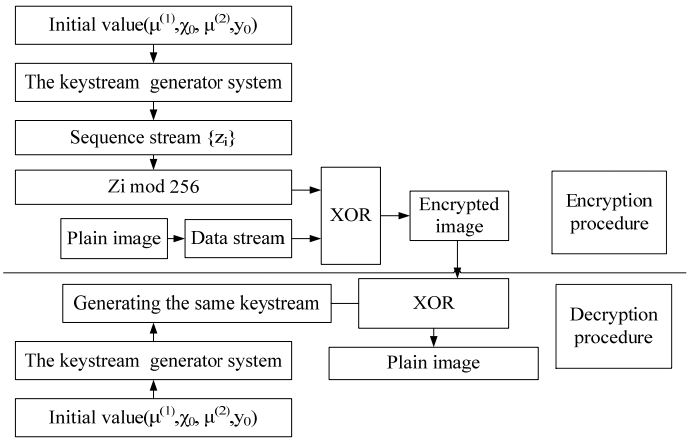

Figure 3. Chaotic encryption algorithm based on coupled chaotic maps.

III. SECURITY ANALYSIS AND TEST RESULTS

In this section, the performance of the proposed image encryption scheme is analyzed in detail. We discuss the security analysis of the proposed image encryption scheme including some important ones like statistical sensitivity, key sensitivity analysis, key space analysis etc. to prove the proposed cryptosystem is secure against the most common attacks.

A. Visual Testing

A number of images are encrypted by the proposed method, and visual test is performed. Two examples are shown in Fig. 4 (a) and Fig. 4 (c), where each image is in 24-bit color with 256x256 pixels. By comparing the original and the encrypted images in Fig. 4, there is no visual information observed in the encrypted image, and the encrypted images are visual indistinguishable even with a big difference in the color tone found in the original images.

In order to further demonstrate the effectiveness of our scheme, some more sophisticated tests suggested in [10, 11] have been carried out and the results are to be explained in the followings.

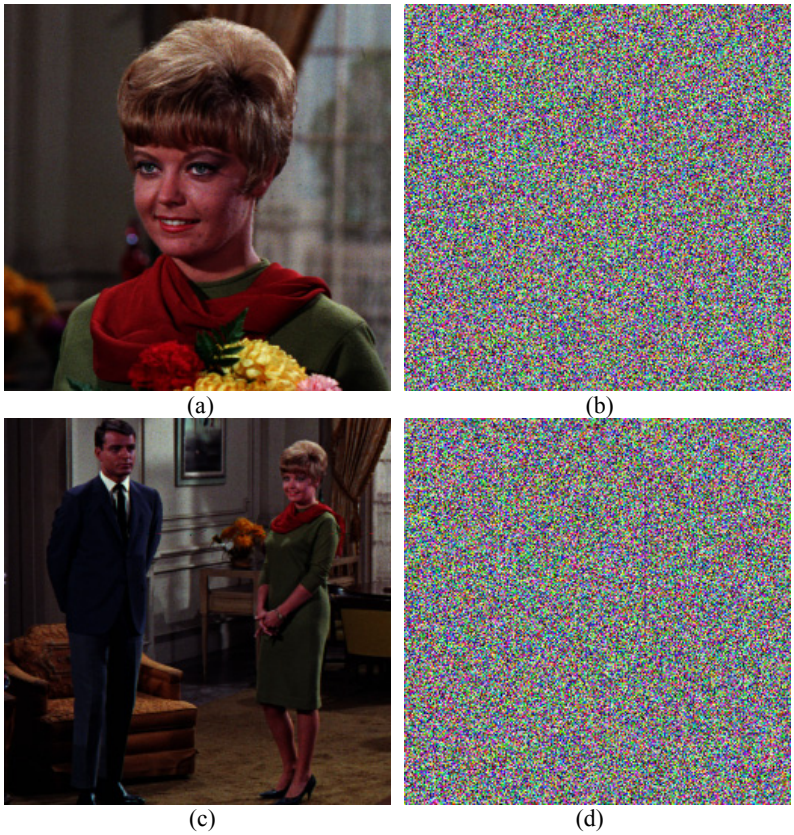

Figure 4. Frame (a) and (c) respectively, show the original images of Girl and Couple. Frame (b) and (d) respectively, show the encrypted images of the plain images shown in frame (a) and (c) using the secret key'4000000000000, 1C28F5C28F5C,3F851EB851EB8, 333333333333 '(in hexadecimal).

B. Statistical Analysis

In order to resist the statistical attacks, the encrypted images should possess certain random properties. We have performed statistical analysis by calculating the histograms, the correlations of two adjacent pixels in the encrypted images and the correlation coefficient for several images and its corresponding encrypted images of an image database. A detail study has been undergone and the results are summarized as followings. Different images have been tested, and similar results are obtained. However, due to the page limit, only the results for the Girl. (Fig. 4(a)) are used for illustration.

(a) Histogram Analysis

In the experiments, the original image and its corresponding encrypted image are shown in Fig. 4 (a) and Fig. 4 (b), and their histograms of red, blue and green channels are shown in Fig. 5. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. Hence the encrypted image does not provide any clue to employ any statistical attack on the proposed image encryption procedure, which makes statistical attacks difficult. Experiments on various images have shown similar results. These properties tell that the proposed cryptosystem has high security against statistical attacks.

Compared with Fig. 1 in Ref.13, our results are more persuasive. In the plain image, some gray-scale values in the range [0, 255] are not existed, but every gray-scale value in the range [0, 255] are existed and uniformly distributed in the encrypted image. In the Fig. 1 in Ref.13,

some gray-scale values are still not existed in the encrypted image although the existed gray-scale values are uniformly distributed. Different images have been tested by the proposed image encryption procedure, and the same property is obtained, which also shows that the proposed chaos-based PRKG can generate chaotic sequences with good pseudo-random properties.

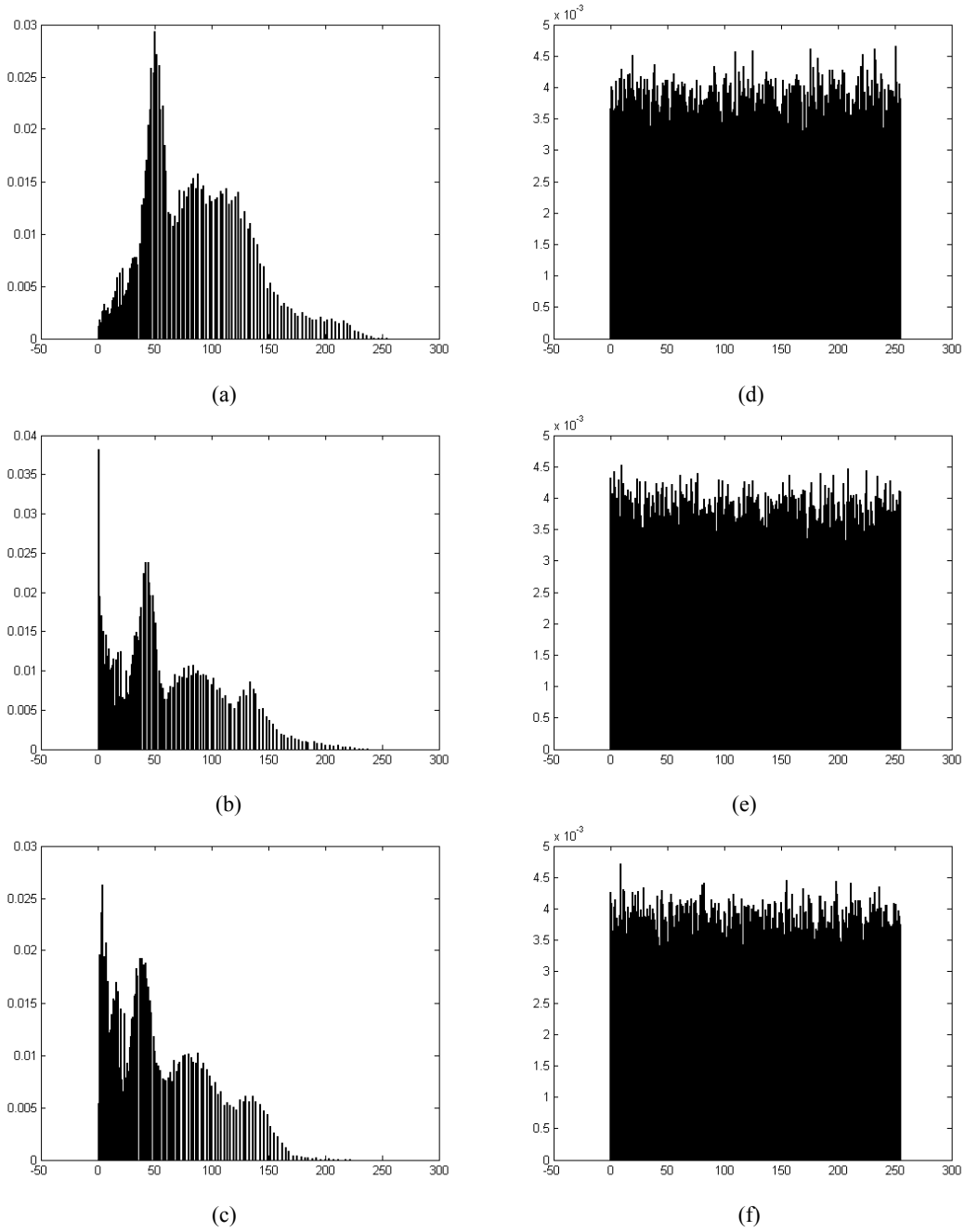

Figure 5. Histogram analysis: Frames (a), (b) and (c) respectively, show the histograms of red, green and blue channels of the plain image shown in Fig. 4 (a). Frames (d), (e) and (f) respectively, show the histograms of red, green and blue channels of the encrypted image shown in Fig. 4 (b).

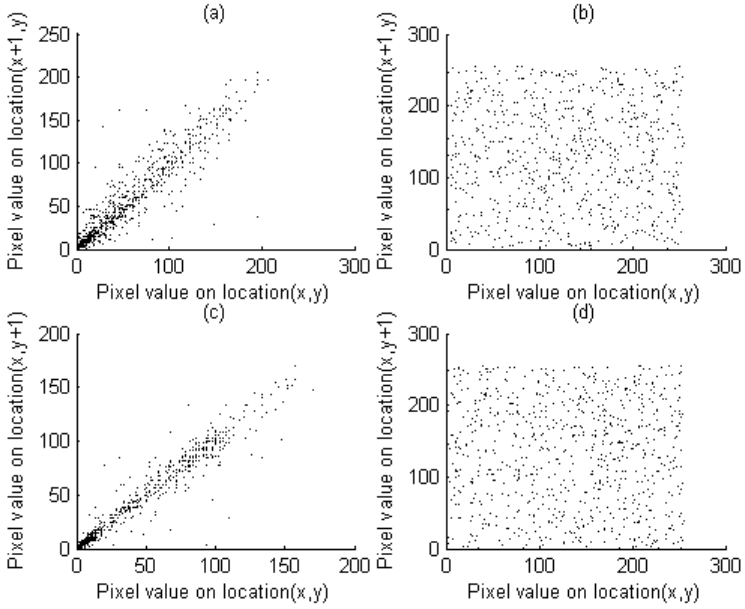

Figure 6. Correlation of two adjacent pixels: Frames (a) and (b) respectively, show the distribution of two horizontally adjacent pixels in the plain and encrypted images shown in Fig. 4 (a) and Fig. 4 (b). Frames (c) and (d) respectively, show the distribution of two vertically adjacent pixels in the plain and encrypted images shown in Fig. 4 (a) and Fig. 4 (b).

(b) Correlation Coefficient Analysis

In order to test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels in the several images and their encrypted images, we also take Girl (Fig. 4 (a)) for example. In Fig. 6, we have shown the distribution of two adjacent pixels in the original and encrypted images shown in Fig. 4 (a) and Fig. 4 (b). Particularly, in Frames (a) and (b), we have depicted the distributions of two horizontally adjacent pixels in the original and encrypted images respectively. Similarly, in Frames (c) and (d) respectively, the distributions of two vertically adjacent pixels in the original and encrypted images have been depicted.

Compared with Fig. 2 in Ref.13, distribution of two adjacent pixels are more uniform in our results, but in the Fig. 2 in Ref.13, distribution displays concentrated trend. Moreover, we have also calculated the correlation between two vertically as well as horizontally adjacent pixels in the original encrypted images, using the following formula referred in Ref.13.

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^{\,2} - (\sum_{j=1}^{N} x_j)^2) \times (N\sum_{j=1}^{N} y_j^{\,2} - (\sum_{j=1}^{N} y_j)^2)}} \quad (8)$$

Where x and y are the gray-scale values of two adjacent pixels in the image and N is total number of pixels selected from the image for the calculation. In the Table 1, we have given the correlation coefficients for the original and encrypted images shown in Fig. 4 (a) and Fig. 4 (b) respectively. In the Fig. 6 and Table 1, it is clear that the two adjacent pixels in the original image are highly correlated, but there is negligible correlation between the two adjacent pixels in the encrypted image.

Additionally, we have also done extensive study of the correlation between image and its corresponding encrypted image by using the proposed encryption algorithm. We have used the USC-SIPI image database which is referred in Ref.13 (freely available at http://sipi.usc.edu/database/).

The secret key ’4000000000000, 1C28F5C28F5C, 3F851EB851EB8, 333333333333 ’(in hexadecimal) has been used for encryption process. Results are shown in the Table 2. The correlation coefficient is very small which implies that no correlation exists between original and its corresponding encrypted images. Compared with Table3 in Ref.13, the correlation coefficient between original and its corresponding encrypted images are generally smaller in our results.

Table 1. Correlation coefficients for the two adjacent pixels in the original and encrypted images shown in Fig. 4.

	Original image (Fig.4(a))	Encrypted image (Fig.4(b))
Horizontal	0.9635	-0.0030
Vertical	0.9711	-0.0028

Table 2. Correlation coefficients between the image and corresponding encrypted image for a number of images of the USC-SIPI image database. The encryption has been done using the secret key '4000000000000, 1C28F5C28F5C, 3F851EB851EB8, 333333333333 '.

File name	File description	Size	Type	Correlation coefficient between the image and corresponding encrypted image	Correlation coefficient for the two adjacent pixels in the encrypted image
4.1.01	Girl	256x256	Color	-0.000492	-0.002887
4.1.02	Couple	256x256	Color	-0.001949	-0.002184
4.1.03	Girl	256x256	Color	0.001619	-0.000796
4.1.04	Girl	256x256	Color	0.001906	-0.003210
4.1.05	House	256x256	Color	0.001563	-0.001986
4.1.06	Tree	256x256	Color	-0.001921	-0.003900
4.1.07	Jelly beans	256x256	Color	0.000114	-0.002231
4.1.08	Jelly beans	256x256	Color	0.002656	-0.002368
4.2.01	Splash	512x512	Color	0.001096	-0.001326
4.2.02	Girl(Tiffany)	512x512	Color	-0.001220	-0.002239
4.2.03	Baboon	512x512	Color	0.000744	-0.000542
4.2.04	Girl(lenna)	512x512	Color	0.001857	-0.000983
4.2.05	Airplane(F-16)	512x512	Color	0.001911	-0.001005
4.2.06	Sailboat on lake	512x512	Color	0.002089	0.000037
4.2.07	Peppers	512x512	Color	0.002248	-0.001883
House	House	512x512	Color	0.000607	-0.000728
5.1.09	Moon surface	256x256	Gray	0.000265	-0.001291
5.1.10	Aerial	256x256	Gray	0.004396	-0.002667
5.1.11	Airplane	256x256	Gray	0.007487	-0.000216
5.1.12	Clock	256x256	Gray	0.014194	-0.002033
5.1.13	Resolution chart	256x256	Gray	0.006588	0.001655
5.1.14	Chemical plant	256x256	Gray	0.000024	-0.003028
5.2.08	Couple	512x512	Gray	0.003597	-0.000508
5.2.09	Aerial	512x512	Gray	0.003001	-0.002298
5.2.10	Stream and bridge	512x512	Gray	0.002980	-0.000530
7.1.01	Truck	512x512	Gray	0.001955	-0.001081
7.1.02	Airplane	512x512	Gray	0.003604	-0.001460
7.1.03	Tank	512x512	Gray	0.002931	0.000002
7.1.04	Car and APCs	512x512	Gray	0.001468	-0.001481
7.1.05	Truck and APCs	512x512	Gray	0.004383	-0.001513
7.1.06	Truck and APCs	512x512	Gray	0.003054	-0.002319
7.1.07	Tank	512x512	Gray	-0.000167	-0.002164
7.1.08	APC	512x512	Gray	0.000198	-0.001414
7.1.09	Tank	512x512	Gray	0.003317	-0.002334
7.1.10	Car and APCs	512x512	Gray	0.000862	-0.003146
boat.512	Fishing Boat	512x512	Gray	-0.000342	0.000087
elaine.512	Girl(Elaine)	512x512	Gray	0.002869	-0.001650
gray21.512	21 level step wedge	512x512	Gray	0.001652	-0.000524
numbers.512	256 level test	512x512	Gray	0.001638	-0.002177
ruler.512	Pixel ruler	512x512	Gray	0.000079	-0.000790
5.3.01	Man	1021x1024	Gray	0.000413	-0.000102
5.3.02	Airport	1021x1024	Gray	0.001564	-0.000221
7.2.01	Airplane	1021x1024	Gray	0.001389	0.000430
testpat.1k	General test pattern	1021x1024	Gray	0.001466	-0.000247

C. Sensitivity Analysis

An encryption scheme has also to be key-sensitive, meaning that a tiny change in the key will cause a significant change in the output. In our tests, we use the fixed initial value 'χ_0=1C28F5C28F5C, y_0=333333333333', changing the system parameter '$\mu^{(1)}$, $\mu^{(2)}$'with a single bit. We know that the system parameter can be any value in the finite area $3.569945<\mu\leq4$, thus we can provide $\mu^{(1)}$ and $\mu^{(2)}$ with the same value. The key sensitivity test is performed in detail according to the following steps:

(1) First, a 256x256 image (Fig. 7 (a)) is encrypted by using the test key1 '$\mu^{(1)}$=3F9F6C38FB143, $\mu^{(2)}$ =3F9F6C38FB143' (in hexadecimal), and its corresponding encrypted image is referred as encrypted image A (Fig. 7 (b)).

(2) Then, the least significant bit of the key is changed, so that the original key becomes key2 '$\mu^{(1)}$=3F9F6C38FB144, $\mu^{(2)}$ =3F9F6C38FB144', which is used to encrypt the same image, and its corresponding encrypted image is referred as encrypted image B (Fig. 7 (c)).

(3) Again, the same image is encrypted by the key3 '$\mu^{(1)}$=3FAF6C38FB143, $\mu^{(2)}$ =3FAF6C38FB143', and its corresponding encrypted image is referred as encrypted image C (Fig. 7 (d)).

(4) Finally, the above three encrypted images A, B and C, encrypted by the three slightly different keys, are compared.

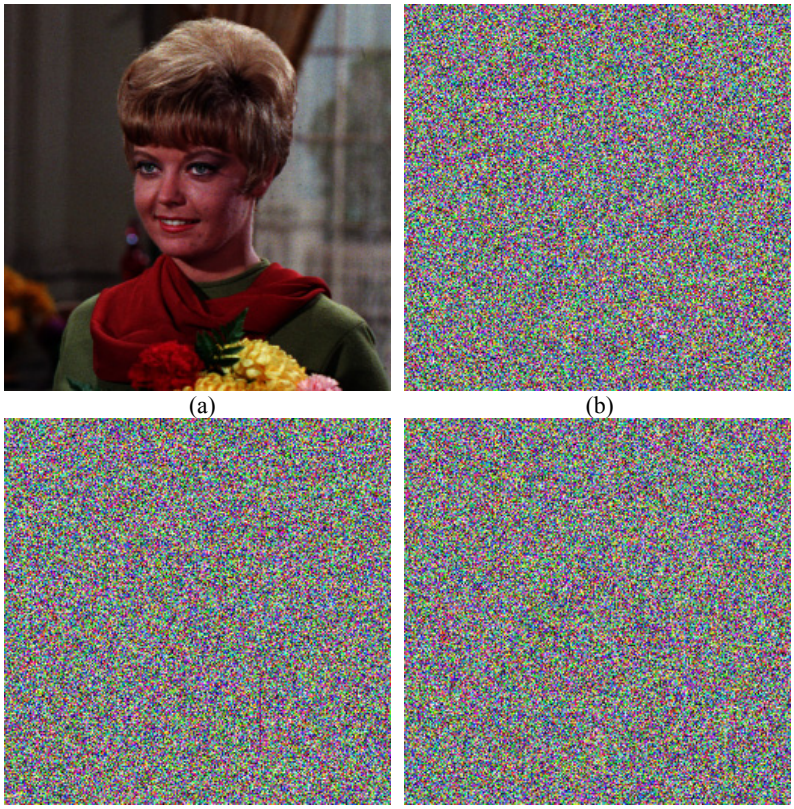

Figure 7. Key sensitivity test 1: Frame (a): plain image; Frame (b): encrypted image A by key1 '$\mu^{(1)}$=3F9F6C38FB143, $\mu^{(2)}$ =3F9F6C38FB143'; Frame (c): encrypted image B by key2 '$\mu^{(1)}$=3F9F6C38FB144, $\mu^{(2)}$ =3F9F6C38FB144'; Frame (d): encrypted image C by key3 '$\mu^{(1)}$=3FAF6C38FB143, $\mu^{(2)}$ =3FAF6C38FB143'.

Table 3. Correlation coefficients between the plain image and the three different encrypted images obtained by using slightly different secret keys.

Image 1	Image 2	Correlation coefficient
Plain image (Fig.7 (a))	Encrypted image A（Fig.7 (b)）	-0.005490
Plain image(Fig.7 (a))	Encrypted image B（Fig.7 (c)）	0.003207
Plain image(Fig.7 (a))	Encrypted image C（Fig.7 (d)）	0.001584

Table 4. Correlation coefficients between the corresponding pixels of the three different encrypted images obtained by using slightly different secret key of an image.

Image 1	Image 2	Correlation coefficient	Difference pixels (mean NPCR)
Encrypted image A（Fig.7 (b)）	Encrypted image B（Fig.7 (c)）	0.000246	99.611%
Encrypted image B（Fig.7 (c)）	Encrypted image C（Fig.7 (d)）	0.001116	99.623%
Encrypted image C（Fig.7 (d)）	Encrypted image A（Fig.7 (b)）	-0.000474	99.605%

For comparison, we use the same ways which is referred in Ref.13, using the same formula as given in Eq.8 except that in this case x and y are the values of corresponding pixels in the two encrypted images to be compared. In table 3 and 4, as can be seen, the correlation between a plain image and the corresponding encrypted images is negligible around zero, which shows that the plain image is nearly independent from the encrypted images. This is consistent with the perfect security defined by Shannon [27]. Similarly, the correlation between different encrypted images is also negligible around zero, which shows that the encrypted images are independent from each other. We have measured the number of pixel change rate (NPCR) of two cipher images with only one bit difference in the keys. In Table 4, it can be observed that the values are very close to the expected value of pixel difference on two randomly generated images (99.609375%). We also obtained NPCR for a large number of images by using our encryption scheme, and found the same results that the encryption scheme is very sensitive with respect to small changes in the key.

Moreover, if we use a trivially modified key to decrypt the ciphered image, then the decryption should not succeed. Figure 8 has verified this, where the image encrypted by the key1 was not be correctly decrypted by using the key2 and key3. Here, there is only one bit difference between the three keys explained before. Those results clearly show high key-sensitivity of the proposed chaotic encryption algorithm.

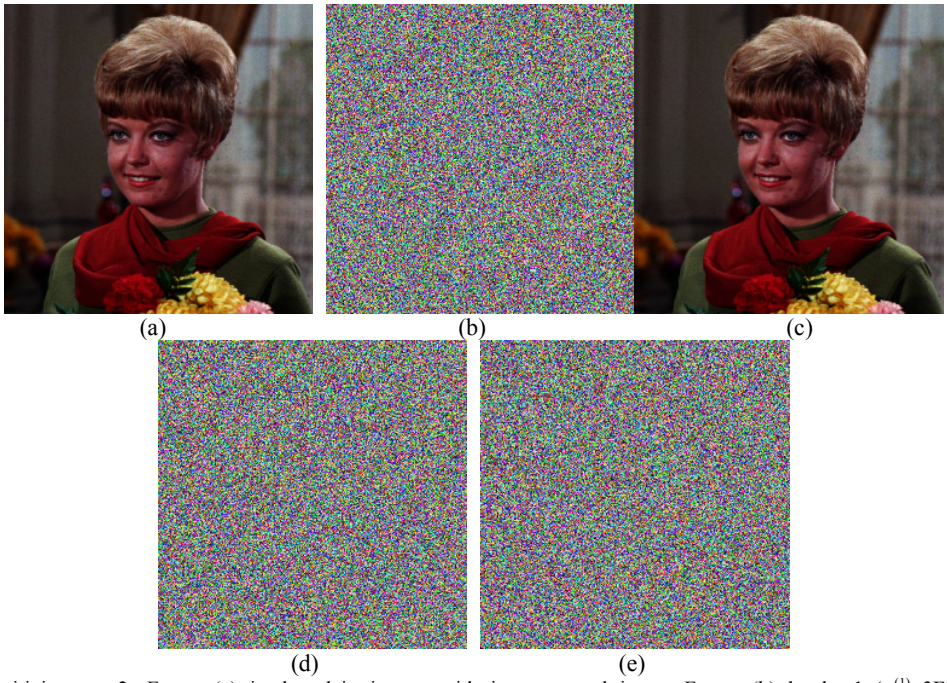

Figure 8. Key sensitivity test 2: Frame (a) is the plain image, with its encrypted image Frame (b) by key1 '$\mu^{(1)}$=3F9F6C38FB143, $\mu^{(2)}$ =3F9F6C38FB143'. Frame (c), (d), and (e) respectively, show the decrypted images by the key1 '$\mu^{(1)}$=3F9F6C38FB143, $\mu^{(2)}$ =3F9F6C38FB143', key2 '$\mu^{(1)}$=3F9F6C38FB144, $\mu^{(2)}$ =3F9F6C38FB144', and key3 '$\mu^{(1)}$=3FAF6C38FB143, $\mu^{(2)}$ =3FAF6C38FB143' to decrypt encrypted image Frame (b).

D. Key Space Analysis

Key space size is the total number of different keys that can be used in the encryption. Cryptosystem is completely sensitive to all secret keys. A good encryption algorithm should not only be sensitive to the cipher key, but also the key space should be large enough to make brute-force attack infeasible. If the precision is 10^{-15}, the key space size for initial conditions and control parameters is over than 2^{196}. Apparently, the key space is sufficient for reliable practical use.

E. Time Analysis

All the security analysis has been done on MATLAB 7.0 by AMD Athlon(tm) 64 X2 Dual Core processor 3800+ 2.0GHz personal computer. We also do the time analysis on it, but not ideal. The keysteam generation system consumes longer time. Considering that the two chaotic logistic maps are suitable for parallel computing in hardware, 64-bit precision representation with fixed point arithmetic is assumed, and a fast throughput and facilitate VLSI architecture is implemented on ALTERA QUATUS II 5.0. The keystream output speed is up to 571.429 Mbps [28], which is strongly suitable for the use of most of real-time video and audio applications.

IV. CONCLUSIONS

In this paper, an image encryption scheme based on coupled chaotic logistic maps is proposed. The system is in a stream-cipher architecture, where the PRKG is formed by two chaotic maps, serving the purpose of stream generation and random mixing, respectively. It is found that such a design can enhance the randomness, even under finite precision implementation. A detailed statistical analysis on the proposed encryption scheme is given. From the experimental results, it is concluded that it outperforms existing schemes, both in terms of speed and security. Having a high throughput, the proposed system is ready to be applied in fast real time encryption applications.

ACKNOWLEDGEMENTS

The work was supported by the National Basic Research Program of China (Grant No. 2006CB303104) and the National Natural Science Foundation of China (Grant No. 40871200).

REFERENCES

[1] B. Hao, *Starting with parabolas: an introduction to chaotic dynamics*, Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993.
[2] R. Brown, L.O. Chua, "Clarifying chaos: examples and counterexamples," *Int. J. Bifurcat Chaos*, vol. 6, pp. 219–242, 1996.
[3] J. Fridrich, "Symmetric ciphirs based on two-dimensional chaotic maps," *Int. J. Bifurcat Chaos*, vol. 8, pp. 1259–1284, 1998.
[4] S. Li, Q. Li, W. Li, X. Mou, Y. Cai, "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding," *IMA Int Conf Crypt & Coding*, vol. 2260, pp. 205–221, 2001.
[5] B. Schneier, *Applied Cryptography–Protocols, Algorithms, and Source Code in C*, 2nd edition, John Wiley & Sons, Inc., New York, 1996.
[6] J. Daemen, B. Sand, V. Rijmen, *The Design of Rijndael: AES–The Advanced Encryption Standard*, Springer-Verlag, Berlin, 2002.
[7] S. Li, Q. Li, X. Mou, Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," *LNCS* 2247,

pp. 316–329, 2001.
[8] S. Li, X. Zheng, "Cryptanalysis of a chaotic image encryption method," *in: Proceedings of the IEEE International Symposium on circuits and systems*, Scottsdale, AZ, USA, 2002
[9] K.W. Wong, S.W. Ho, C.K. Yung, "A chaotic cryptography scheme for generating short ciphertext," *Phys. Lett. A*, vol. 310, pp. 67–73, 2003.
[10] G. Chen, Y. Mao, C.K. Chui, "A symmetric image encryption based on 3D chaotic maps," *Chaos Solitons Fractals*, vol. 21, pp. 749–761, 2004.
[11] Y.B. Mao, G. Chen, S.G. Lian, "A novel fast image encryption scheme based on the 3D chaotic baker map," *Int. J. Bifurcat Chaos*, vol. 14, pp. 3613–3624, 2004.
[12] S.G. Lian, J. Sun, Z. Wang, "A block cipher baser on a suitable use of chaotic standard map," *Chaos Solitons Fractals*, vol. 26, pp. 117–129, 2005.
[13] N.K. Pareek, V. Patidar, K.K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, pp. 926–934, 2006.
[14] T. Xiang, X. Liao, G. Tang, Y. Chen, K.W. Wong, "A novel block cryptosystem based on iterating a chaotic map," *Phys. Lett. A*, vol. 349, pp. 109–115, 2006.
[15] H.S. Kwok, W.K.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos Solitons Fractals*, vol. 32, pp. 1518–1529, 2007.
[16] T. Xiang, K.W. Wong, X. Liao, "A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map," *Phys. Lett. A*, vol. 364, pp. 252–258, 2007.
[17] P. Li, Z. Li, W.A. Halang, G. Chen, "A stream cipher based on a spatiotemporal chaotic system," *Chaos Solitons Fractals*, vol. 32, pp. 1867–1876, 2007.
[18] J. Wei, X. Liao, K.W. Wong, T. Zhou, "Cryptoanalysis of a cryptosystem using multiple one-dimensional chaotic maps," *Commun. Nonlinear Sci. Numer. Simul*, vol. 12, pp. 814–822, 2007.
[19] K.W. Wong, B.S.H. Kwok, W.S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, pp. 2645–2652, 2008.
[20] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan. "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos Solitons Fractals*, vol. 35, pp. 408–419, 2008.
[21] N.K. Pareek, Vinod Patidar, K.K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. A*, vol. 309, pp. 75–82, 2003.
[22] N.K. Pareek, Vinod Patidar, K.K. Sud, "Cryptography using multiple one-dimensional chaotic maps," *Commun. Nonlinear Sci. Numer. Simu*l, vol.10, pp. 715–723, 2005.
[23] M.A. Jafarizadeh, S. Behnia, S. Khorram, H. Nagshara, "Hierarchy of chaotic maps with an invariant measure," *J Stat Phys*, vol. 104, pp. 1013–1028, 2001.
[24] M.A. Jafarizadeh, S. Behnia, "Hierarchy of chaotic maps with an invariant and their coupling," *Physica D*, vol. 159, pp.1–21, 2001.
[25] M.S. Baptista, "Cryptography with chaos," *Phys. Lett. A*, vol. 240, pp. 50–54, 1998.
[26] T. Geisel, V. Fairen, "Statistical Properties of Chaos in Logistic Map," *Phys. Lett. A*, vol. 105, pp. 263-266, 1984.
[27] C. Shannon, "Communication theory of secrecy systems," *Bell Syst Tech J*, vol. 28, pp. 656–715, 1949.
[28] S.B. Liu, J. Sun, Z.Q. Xu, Z.H. Cai, "An improved chaos-based stream cipher algorithm and its VLSI implementation", 4th International Conference on Networked Computing and Advanced Information Management, vol.2, Gyeongju, KOREA, 2008.

Shubo Liu received the B.E. degree in electronic technology and the M.S. degree in computer application from Wuhan University (WHU), Hubei, China, in 1993 and 1999, respectively, and he is currently pursuing the Ph.D. degree in communication and information system at WHU.

Since 1993, he has been on the faculty in computer school at WHU, and he is currently an Associate Professor in the Department of Computer Application. His research interests include multimedia information security, and multimedia network communication technology.

Mr. Liu was awarded two scientific and technological progress prizes and one invent patent applying.

Jing Sun received the B.E. degree in information security form Hubei Police University, China, in 2007, and the M.S. degree in computer application form Wuhan University (WHU), China. She is currently pursuing the Ph.D. degree in communication and information system at WHU.

She is a researcher in the Multimedia Information Security of the State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing at WHU. Her research interests include multimedia information security, information theory, and communication networks.

Miss. Sun received the Master First-Level Scholarship (Best Student Award) form WHU, in 2008.

Zhengquan Xu received the B.E. degree in radio technology and information system and M.S. degree in communication and electronic system form Tsinghua University, China, in 1985 and 1988, respectively, and the Ph.D degree in biomedicine engineering form Hong Kong Polytechnic University, in 1998.

From 1988 to 1999, he was on the faculty in the department of Electronics and Information at the Huazhong University of Science and Technology. In 1995, he was selected to the Hong Kong Polytechnic University (HKPU) by the State Education Ministry. During the period, he was selected to Stanford University as a short-term visiting scholar by the "Areas of Excellence" plan of the HKPU. Since 1999, he has been on the faculty in Wuhan University (WHU). He is currently the director of multimedia communication engineering center of state key laboratory of information engineering in surveying, mapping and remote sensing at WHU. He is the expert of government affairs information construction engineering of Wuhan City, and the expert of government affairs information construction engineering of Hubei Province. His research interests include space and multimedia information processing, multimedia information security, and multimedia network communication technology.

Mr. Xu has presided or participated in a variety of more than 20 research projects and was awarded five scientific and technological progress prizes: three Ministerial-level and two Municipal-level awards respectively.