Available online at www.sciencedirect.com
ScienceDirect
Progress in Natural Science 18 (2008) 1299–1304
Progress in Natural Science
www.elsevier.com/locate/pnsc

A video encryption method based on chaotic maps in DCT domain

Shuguo Yang [a,b,*], Shenghe Sun [a]

[a] School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin 150001, China
[b] Qingdao University of Science and Technology, Qingdao 266061, China

Received 17 October 2007; received in revised form 5 May 2008; accepted 28 May 2008

Abstract

This paper proposes a new and secure video encryption method based on chaotic maps in DCT domain, which is quite in keeping with the common ideas and the frequent practices of video encryption. We select the I-frames of the video sequence as encryption objects. First, we introduce two coupling chaotic maps to scramble the DCT coefficients of every original I-frame, and receive the scrambled I-frame. Second, we encrypt the DCT coefficients of the scrambled I-frame using another chaotic map. In the whole process, we use three chaotic maps and five keys; the I-frame is encrypted twice. Finally, we performed several tests and the experimental results have proved our method to be secure and efficient.

Keywords: Video encryption; Chaotic map; I-frame; Scrambling; Video sequence

1. Introduction

With the development of multimedia and network technology, digital TV, video mail, visual telephone, etc. have become more and more popular and now have a widespread and profound influence on our lives. Because video streams are often subject to malicious attacks such as information divulgence, information theft, and data distortion, the security of video stream has become a hot research topic.

Researchers are more and more concerned about encryption algorithms of compressed video based on explosive multimedia applications. Many methods for encrypting and decrypting video data have been proposed. However, there are many drawbacks in the current schemes in respect of security and real-time performance. For example, Tang [1] scrambled the discrete cosine transform (DCT) coefficients of every 8 × 8 video image block; however, the volume of the video image increases greatly and the method is unable to resist the known-plaintext attack. Qiao et al. [2] presented a new encryption algorithm for MPEG video based on the statistical characteristics of MPEG. This algorithm can cut down 47% resources and time, but it does not consider the correlative information of the video frames. Thus potential attackers can make a success once they obtain some correlative information. Alattar and Al-Regib [3] proposed a selective encryption technique that selects various I-frames and encrypts them. This method is secure and can resist the known-plaintext attack. Wu and Moo [4] presented a kind of sequence encryption method based on the embedded conditional entropy coding of wavelet coefficients (ECECOW). This method combines an image compression algorithm with the embedded conditional entropy coding and achieves good security by encrypting part of the compression codes. Romolotti et al. [5] proposed a solution that adopts discrete exponentiation over Galois Fields to encrypt real-time multimedia data. This RPK scheme is simple and secure. The method presented in [6,7] only encrypts the head information of MPEG video. But it is not effective

* Corresponding author. Tel.: +86 532 68822651.
E-mail address: ysg_2005@hotmail.com (S. Yang).

1002-0071/$ - see front matter © 2008 National Natural Science Foundation of China and Chinese Academy of Sciences. Published by Elsevier Limited and Science in China Press. All rights reserved.
doi:10.1016/j.pnsc.2008.05.009

because the head information only includes standard information and an attacker can decrypt it easily. Yen [8] made the gray scale of every pixel of the video frame NOR a secret key which is generated by a chaotic map. His method describes a system structure enforced by hardware but without any estimation of the time cost. Sobhy [9] encrypted video information by Lorenz chaos system, but the implementation of his method is inefficient and slow. Chiaraluce et al. [10] presented a novel chaotic algorithm for video encryption that encrypts the DC and AC coefficients of the I-frame, the sign of the AC coefficients of the P-frame and the motion vectors. It is secure and can easily be implemented in real-time. Yuan et al. [11] presented a chaotic selective encryption algorithm for compressed video (CSECV). They adopted the chaos method as a pseudorandom sequence generator, and combined a dissymmetric key system with the sequence cryptography system. In a series of tests including cryptanalysis, algorithm evaluation and comparison with other algorithms, CSECV has shown significant advantages in security, real-time performance and flexibility of implementation. Zhang [12] proposed a method that adopts the chaos method as a pseudorandom sequence generator and combined it with the merits of some other algorithms. It has been applied to MPEG2 algorithm and wavelet-based video compression algorithms. The former can be done in real-time, whereas the latter can reach a high compression ratio. As software, this method is secure and fast.

In our scheme reported here, we encrypt and decrypt the I-frames of the compressed video to create the same effect on the B-frames, P-frames, and entire video. In Section 2, we select our encryption objects. The double coupling logistic maps are presented in Section 3. We describe in detail the scrambling method for the DCT coefficients of the I-frame based on the chaotic maps in Section 4. In Section 5, the encryption method for the DCT coefficients of the I-frame is presented. Finally, we present our conclusions based on the experiments in Section 6.

2. Selecting the encryption frames

A compressed video sequence M consists of three parts: head information of the video stream, motion vector data stream and DCT data stream. There are three kinds of frames in the video stream M, namely I-frame, B-frame and P-frame. These frames are freely arranged by the encoder in the form: I P B B P B B..... Their relationship can be shown in Fig. 1.

The codes of the I-frames do not refer to any other frame and they provide the access points of the image code data. I-frames are also the beginning of decodes and are compressed based on common methods. P-frames are compressed effectively and can be predicted by the former I-frames and P-frames. B-frames are greatly compressed and cannot provide reference to the later frames. Obviously, I-frames as the beginning of decodes are more important than the other frames. The encryption of an I-frame can greatly influence the relevant B-frames, P-frames and entire video, so we scramble I-frames and encrypt them in our encryption scheme. The later tests prove this idea to be effective.

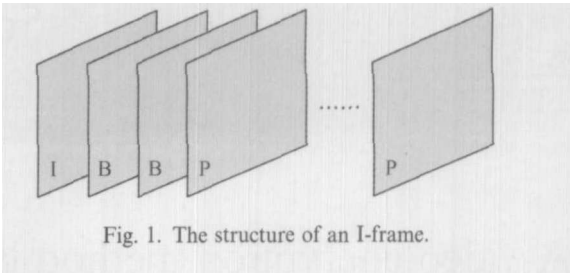

Fig. 1. The structure of an I-frame.

3. Double coupling logistic maps

Chaos is a kind of complex dynamic behavior of nonlinear systems. The logistic chaotic map is a discrete iteration system which can be formulated as:

$$x_{n+1} = \mu x_n(1 - x_n),\ n = 0, 1, 2, \ldots$$

where x_0 is the initial value of the iteration system, x_n is the value of the chaotic sequence, parameter μ can control the behavior of the non-linear system, and $0 \leqslant x_n \leqslant 1$, $0 < \mu \leqslant 4$. The map is chaotic when $3.5699456\cdots \leqslant \mu \leqslant 4$.

In order to enhance the random and encryption characters of the chaotic sequence, we adopt two logistic maps and mix them by controlling the parameters of each other. The coupling Logistic maps are given below

$$\begin{cases} x_{n+1} = \mu_x x_n(1 - x_n) \\ y_{n+1} = \mu_y y_n(1 - y_n) \end{cases} \tag{1}$$

where μ_x and μ_y are parameters, and x_n and y_n are the values of the chaotic sequences. The value of parameter μ_x is 3.9 or 3.9888 and the value of parameter μ_y is 3.944444 or 4.0. The parameters are altered according to the following equations:

$$\mu_x = \begin{cases} 3.9 & 0 < y_j \leqslant 0.5 \\ 3.9888 & 0.5 < y_j \end{cases} \qquad \mu_y = \begin{cases} 3.9444 & 0 < x_i \leqslant 0.5 \\ 4.0 & 0.5 < x_i \end{cases} \tag{2}$$

From Eqs. (1) and (2), we can produce the chaotic sequences $\{x_1, x_2, \ldots, x_m\}$ and $\{y_1, y_2, \ldots, y_n\}$ [13].

4. The scrambling method for an I-frame based on chaotic maps

Suppose one of the original I-frames in the compressed MPEG video data stream M is I_0. After being transformed by DCT, I_0 can be denoted as $D(I_0)$ which is as follows:

$$D(I_0) = \bigcup_{i,j} D(i,j)\ (1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant n) \tag{3}$$

where (i,j) denotes the position of a pixel point in $D(I_0)$; $D(i,j)$ denotes the DCT coefficient of the point (i,j).

The process of scrambling $D(I_0)$ is described below.

(i) Setting the initial values of the chaotic systems in Eq. (1) to x_0 and y_0, respectively, we can produce two chaotic sequences $x_1, x_2, \ldots, x_a$ and $y_1, y_2, \ldots, y_a$ $(a = \max\{m,n\})$.Then we select two chaotic sequences $x_1, x_2, \ldots, _m$ and $y_1, y_2, \ldots, y_n$ and arrange the two chaotic sequences separately by magnitude, and obtain the sequences $x'_1, x'_2, \ldots, x'_m$ and $y'_1, y'_2, \ldots, y'_n$. Each x_i $(i = 1,2,\ldots,m)$ corresponds to an integer w_{x_i} $(\in \{1,2,\ldots,m\})$, which is the order of x_i in the new sequence $x'_1, x'_2, \ldots, x'_m$. At the same time, each $y_j (j = 1,2,\ldots,n)$ corresponds to an integer w_{y_j} $(\in\{1,2,\ldots,n\})$, so that each (x_i, y_j) corresponds to (w_{x_i}, w_{y_j}).

(ii) Disordering the coefficients of $D(I_0)$ Each coefficient $D(i,j)$ of $D(I_0)$ in the original frame I_0 corresponds to (x_i, y_j), and each (x_i, y_j) corresponds to (w_{x_i}, w_{y_j}), therefore each (i,j) corresponds to (w_{x_i}, w_{y_j}). We replace coefficient $D(i, j)$ by coefficient $D(w_{x_i}, w_{y_j})$, and then we obtain the scrambled $D_1(I_0)$.

In the process mentioned above, the initial values of the chaotic maps in Eq. (1) can be regarded as the secret keys $(K_1 = x_0, K_2 = y_0)$. Because we change the position of each coefficient $D(i,j)$ without bringing any change in the magnitude of each $D(i,j)$ of $D(I_0)$, the retrieval of I_0 is successful.

5. The encryption method for an I-frame based on a chaotic map

The process of encrypting the $D_1(I_0)$ of the original I-frame is

(i) After arranging the DCT coefficients of $D_1(I_0)$ using the row scan method, we obtain the coefficient sequence $d_1(i)$ $(i = 1,2,\ldots,mn)$.

(ii) We produce a chaotic sequence $x(i)$ $(i = 1,2,\ldots,mn)$ using the following equation:

$$x(i+1) = 1 - \mu x^2(i) \tag{4}$$

where $x(0)$ is a preset initial value, $x(i) \in (-1,1)$ $(i = 1,2, \ldots,mn)$, and μ is a parameter. The map can be chaotic if the parameter μ is selected properly.

(iii) In order to make the DCT coefficients of $D_1(I_0)$ change adaptively, we adopt the following equation to modify every coefficient of $D_1(I_0)$

$$d'_1(i) = d_1(i)(1 + x'(i)) \tag{5}$$

where $x'(i)$ is derived from $x(i)$ when we set the number of significant figures of $x(i)$ to λ, $d_1(i)$ is the original DCT coefficient of $D_1(I_0)$, and $d'_1(i)$ is the new DCT coefficient of $D'_1(I_0)$.

(iv) After transforming $D'_1(I_0)$ using IDCT based on coefficient $d'_1(i)$, we obtain the encrypted I-frame I'_0.

In the process mentioned above, we introduce three keys $(K_3 = \mu, K_4 = x(0), K_5 = \lambda)$ again, then we obtain five keys $(K_1, K_2, \ldots, K_5)$. Because the chaotic sequence is hard to predict and the ranges of these keys are very wide, searching the keys is almost impossible. At the same time, the changes in the I-frame can greatly influence the B-frames and P-frames, so video decryption is very difficult and thus scrambling and encrypting video is very effective.

The flowchart of the process of scrambling and encrypting an I-frame is presented in Fig. 2.

The process of decrypting an I-frame is the reverse of the process described above.

6. Experimental results

To test our encryption method for security and robustness, we conducted many experiments on the video sequence M with 200 I-frames whose sizes are 288 × 352. We randomly chose an I-frame I_0 from M, and set x_0 to 0.111 and y_0 to 0.101 in Eq. (1), and then we obtained the chaotic pairs $(x_i, y_j)(i = 1, 2, \ldots, m, j = 1,2, \ldots, n)$. We rearranged the $D(i,j)$ of $D(I_0)$ according to the method in step (ii) of Section 4, thus obtaining the scrambled $D_1(I_0)$. After setting μ to 1.581 and $x(0)$ to 0.1101 in Eq. (4), we obtained the chaotic sequence $x(i)$ and $x'(i)$ $(i = 1,2, \ldots, mn, \lambda = 3)$, and then calculated $d'_1(i)$ $(i = 1,2,\ldots,mn)$ by Eq. (5) $[d'_1(i)$ is the new DCT coefficient of $D'_1(I_0)]$. We transformed $D'_1(I_0)$ using IDCT based on the new coefficient $d'_1(i)$ to obtain the encrypted I-frame I'_0. We obtained the encrypted video by encrypting every I-frame of the video. A typical original I-frame and its corresponding encrypted I-frame are shown in Figs. 3 and 4.

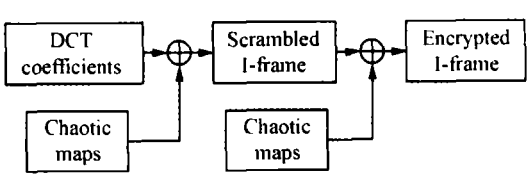

Fig. 2. Scrambling and encrypting an I-frame.

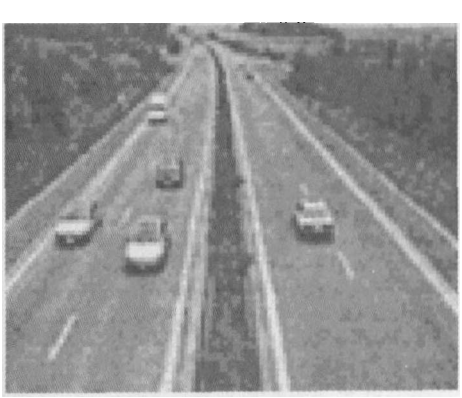

Fig. 3. A typical original I-frame.

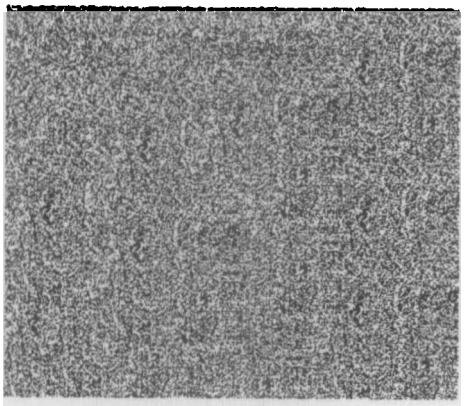

Fig. 4. The encrypted I-frame.

6.1. Test 1. Decryption test

First, we transformed the encrypted I-frame I'_0 (Fig. 4) by DCT to obtain the coefficient $d'_1(i)$ $(i = 1,2,\ldots,mn)$. Second, we set μ to 1.581 and $x(0)$ to 0.1101, calculated the sequence $x(i)$ and $x'(i)$ $(i = 1,2,\ldots,mn,\ \lambda = 3)$ based on Eq.(4), calculated the coefficient $d_1(i)$ according to $d'_1(i)$ and Eq.(5) and then obtained the scrambled $D_1(I_0)$. We processed it according to the inverse process of scrambling I-frames, and then obtained the decrypted I-frame (Fig. 5).

Comparing the decrypted I-frame (Fig. 5) with the original I-frame (Fig. 3), we draw a conclusion that they are almost the same if we adopt the correct keys when decrypting the encrypted frame; that is, the method is secure. In fact, the entire original video can be obtained based on the process above.

6.2. Test 2: distortion test

The distortion of this scheme is also considered. In the whole process of scrambling, encrypting and decrypting the I-frame, scrambling the I-frame is distortion-free, while the distortion brought about by encryption and decryption depends on the DCT.

Comparing the original I-frame (Fig. 3) with the decrypted I-frame (Fig. 5), the distortion rate brought about by the encryption and decryption is 0.1%, which is so small that we can barely see any difference between the original I-frame and the decrypted I-frame. The distortion rates of the different encryption methods are given in Table 1 [14].

Fig. 5. The decrypted I-frame.

Table 1
The distortion rates of different encryption methods

Encryption methods	Distortion rate (%)
Our method	0.1
Real number sequence encryption method	1.3
Magic cube permutation method	1.5
Sign matrix encryption method	1.3

6.3. Test 3: security test

In the process of scrambling and encrypting the I-frame above, we introduced five keys $(K_1, K_2, \ldots, K_5)$. Therefore, we must test the sensitivity of the decryption of an I-frame with respect to each key.

First, we conducted the encrypted I-frame (Fig. 4) when x_0 is 0.1111, y_0 is 0.10101 and other keys (μ, λ and $x(0)$) are correct, we obtained the decrypted I-frame (Fig. 6a).

Second, we set x_0 to 0.111 and y_0 to 0.101 and tested the effect on the decryption with one of the keys μ, λ or $x(0)$ being incorrect.

We conducted the encrypted I-frame (Fig. 4) with $\mu = 1.581001$, $\lambda = 3$ and $x(0) = 0.1101$ according to the process in Test 1, and then we obtained the decrypted frame (Fig. 6b). According to the same process, we obtained the decrypted frame (Fig. 6c) with $\mu = 1.581$, $\lambda = 3$ and $x(0) = 0.110$, and the decrypted frame (Fig. 6(d)) with $\mu = 1.581$, $\lambda = 4$ and $x(0) = 0.1101$.

Comparing the four decrypted I-frames (Fig. 6a–d) with the original I-frame (Fig. 3), we conclude that the decrypted I-frames are very different from the original I-frame if we use erroneous keys which are slightly different from the correct key when we decrypt the encrypted I-frame. That is, if we wish to obtain the correct I-frame information, we must find the correct keys. If every value of the keys μ, λ and $x(0)$ is a double type of decimal fraction, the total range of these three keys is $10^{15} \times 10^{15} \times 10^{15} = 10^{45} \approx 2^{149}$. Searching for these keys is therefore very difficult and the method is thus secure. If we also consider the effect of x_0 and y_0, the total range of the five keys is larger still and the method is even more secure.

From any of the video frames, we can see that the encryption effect of this scheme is very effective, and therefore, the security of the encrypted video is also fine.

6.4. Test 4: correlation of the adjacent pixels

To test the correlation of adjacent pixels, we randomly selected 1820 couples of pixels (horizontal, vertical and diagonal) in the original I-frame and the encrypted I-frame

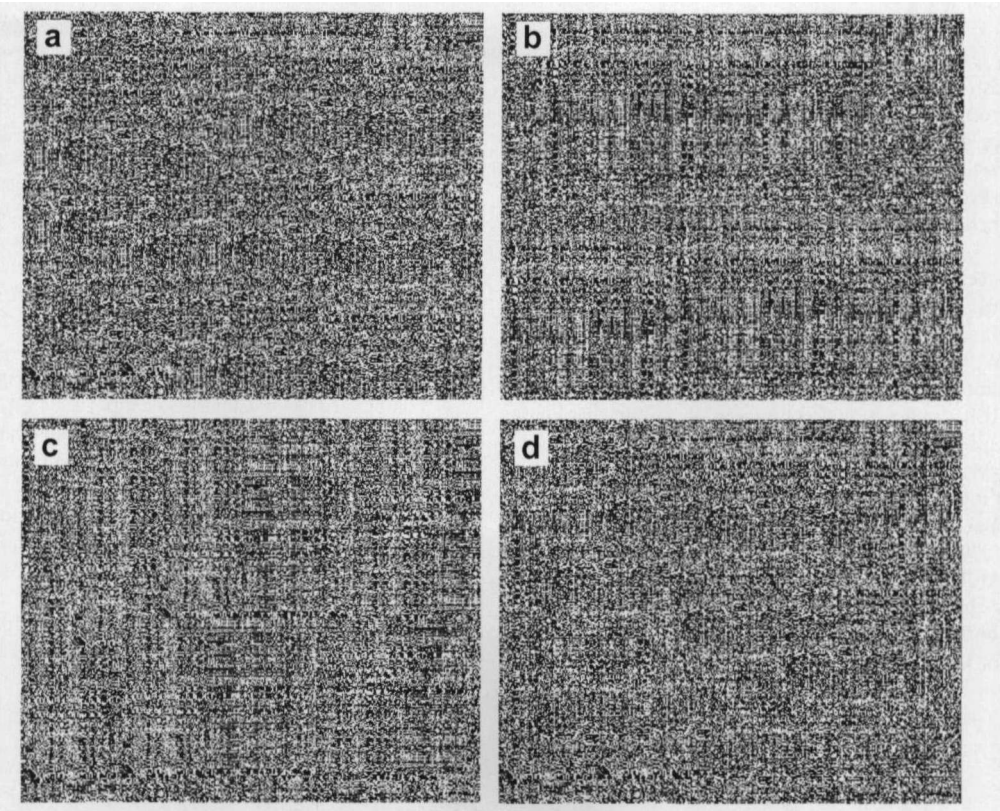

Fig. 6. The decrypted I-frame.

and calculated the correlation coefficients of two adjacent pixels according to the formula which is given:

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)D(y)}} \tag{6}$$

where x and y denote the gray of two adjacent pixels in the I-frame, and r_{xy} denotes the correlation coefficient of two adjacent pixels.

The correlation coefficients of two adjacent pixels in the original I-frame and the encrypted I-frame are listed in Table 2.

From the table above, we can draw a conclusion that adjacent pixels in the original I-frame are highly correlative whereas the correlativity of adjacent pixels in the encrypted I-frame is small. The statistical characteristic of the original I-frame diffuses into the encrypted I-frame.

6.5. Test 5. Time consumption test

We compared our scheme with other common methods with regard to time consumption, and the results are shown in Table 3.

Table 2
The correlation coeffcients of two adjacent pixels in the original I-frame and the encrypted I-frame

Direction	Original I-frame	Encrypted I-frame
Horizontal	0.9671	0.00251
Vertical	0.9655	0.00237
Diagonal	0.9683	0.00198

Table 3
The consumed time of different encryption methods

Encryption methods	Encryption time (s)	Decryption time (s)
Our method	32	32
Real number sequence encryption method	33	33
Magic cube permutation method	33	34
Sign matrix encryption method	31	31

From the above table, we can see that the real-time characteristic of our scheme is better than the others. Our method is thus feasible.

7. Conclusions

The proposed method includes two key operations: scrambling I-frames and encrypting I-frames, and uses three chaotic maps (two coupling chaotic maps and one chaotic map). It has five keys in the whole process which are found to be difficult, and the changes of the I-frames can bring much influence on the whole video. As verified by various test results, this frame encryption method is secure.

Acknowledgements

This project was supported by the Postdoctoral Research Fund of Harbin Institute of Technology (LRB05-061) and Research Fund for Doctors of Qingdao University of Science and Technology.

References

[1] Tang L. Methods for encrypting and decrypting MPEG video data efficiently. In: Proceedings of the fourth ACM International Multimedia Conference. Boston, USA; 1996. p. 219–29.

[2] Qiao L, Nahrstedl K. A new algorithm for MPEG video encryption. In: Proceedings of the first international conference on imaging science, systems and technology. Vegas, Nevada; 1997. p. 21–9.

[3] Alattar AM, Al-Regib GI. Improved selective encryption techniques for secure transmission of MPEG video bit streams. In: Proceedings of ICIP. Kobe, Japan; Apr, 1999. p. 256–60.

[4] Wu XL, Moo PW. Joint image/video compression and encryption via high-order conditional entropy coding of wavelet coefficient. In: Proceedings of IEEE international conference on multimedia computing and systems. Florence, Italy; Jul, 1999. p. 908–12.

[5] Romolotti RG, Mattavelli M. Cryptosystem architectures for very high throughput multimedia encryption. In: Proceedings of the sixth IEEE international conference on electronics, circuits and systems. Pafos, Cyprus; 1999. p. 261–4.

[6] Alattar AM, Al-Regib GI. Evaluation of selective encryption techniques for secure transmission of MPEG compressed bitstreams. In: Proceedings of the IEEE international symposium on circuits and systems. Orlando, USA; Jul 1999. p. 340–3.

[7] Teixeira L, Sarmento L. Secure transmission of MPEG video sources. In: Proceedings of the sixth international workshop on intelligent signal processing and communication systems. Melbourne, Australia; 1998. p. 173–7.

[8] Yen JC, Guo JI. A new chaotic key-based design for image encryption and decryption. In: Proceedings of IEEE international symposium on circuits and systems. Geneva, Switzerland; 2000. p. 49–52.

[9] Sobhy MI, Shehata AR. Chaotic algorithms for data encryption. In: Proceedings of international conference on acoustics, speech and signal processing. USA; 2001. p. 997–1000.

[10] Chiaraluce F, Ciccarelli L, Gambi E, et al. A new chaotic algorithm for video encryption. IEEE Trans Consumer Electron 2002;48(4):838–44.

[11] Yuan C, Zhong YZ, He YW. Chaos based encryption algorithm for compressed video. Chinese J Comput 2004;27(2):257–62, [in Chinese].

[12] Zhang M, Liu ZX, Sun QL, et al. Chaos based video compression and encryption algorithms. Control Eng China 2005;12(5):482–5, [in Chinese].

[13] Zheng DL, Zhao G, Xu GB. Logistic map digital stream chaos singularity terminal and parameters. J Beijing Univ Sci Technol 2002;24(3):350–2, [in Chinese].

[14] Chen QL, Liao XF, Chen Y, et al. Modified image encryption based on chaotic sequences and rublik cube transformation. Comput Eng Appl 2005(22):138–9, [in Chinese].