Efficient video encryption by image key based on hyper-chaos system

Vahid Alirezaei, Moghani Reza
Communication and Information Technology Group
Payame Noor University
PNU Mashad, Iran
{V_alirezaei2007, moghani_reza}@yahoo.com

ABSTRACT: *In this paper, an efficient video encryption scheme is constructed by image key and is based on hyper-chaos system. The chaotic lattices are used to generate pseudorandom sequences and then selected pixel and bitpixel of image key encrypt frame blocks one by one. By iterating chaotic maps for certain times, the generated pseudorandom sequences obtain high initial-value sensitivity and good randomness. The pseudorandom-bits in each lattice are used to select pixel and bitpixel of image key and then encrypt the Direct Current coefficient (DC) and the signs of the Alternating Current coefficients (ACs). Theoretical analysis and experimental results show that the scheme has good cryptographic security and perceptual security, and it does not affect the compression efficiency apparently. These properties make the scheme a suitable choice for practical applications.*

Keywords: Mpeg video, Video Compression, Security, Image Key, Video Encryption, Chaos System

Received: 11 August 2011, Revised 8 October 2011, Accepted 18 October 2011

1. Introduction

The main advantage of a chaotic secure communication system over conventional cryptosystems is that chaotic secure communication systems can often be realized as very simple circuits on a part of a chip [1]. Additionally, the properties of initial-value sensitivity and parameter sensitivity make the initial-value and parameters suitable for encryption keys. Till now, some chaos based data protection means have been proposed, among which, data encryption is the typical one. Data encryption [2] often transforms the original data into an unintelligible form, which protects the confidentiality. According to the properties, the algorithms can be classified into several types, i.e., chaotic switching, chaotic modulation, chaotic stream cipher, chaotic block cipher, and some other encryption algorithms. In chaotic switching [3], two chaotic systems are used to represent binary signals „0 and „1 , respectively. In chaotic modulation [4], chaotic sequence acts as the carrier of the message. In chaotic stream ciphers, a key stream is produced by chaotic sequence generator, which is used to encrypt the plaintext one by one [5], discrete chaotic dynamic system [6, 7], coupled map lattices [8]. Chaotic block ciphers transform the plaintext block by block with chaotic maps. For example, the cipher is constructed based on modified Baker map [9], discrete 2D Baker map [10] or 3D chaotic maps [11]. For the property of easy implementation, chaos has been used to construct the encryption scheme for images or videos data. For example, the cascaded chaos maps are used to construct the stream cipher for image encryption , the discrete Kolmogorov flow map is used to design the parallel image encryption algorithm [12], two chaotic maps are combined to shuffle the image pixels [13], discrete exponential chaotic maps confusion and diffusion properties are improved and used to design the image encryption algorithm [14]. The 2D Baker map is used to construct the block cipher for images [8]. In practice, videos are often compressed in order to save the cost of storage space or transmission loading. Thus, it is more reasonable to encrypt the compressed data. Spatiotemporal chaos system is regarded as a system whit better properties suitable for data protection than 1D chaos system, such as larger parameter space, better randomness and more chaotic sequences, etc. In sequence generation coupled map lattice is adopted as a prototype of a spatiotemporal chaotic system, and multiple pseudorandom-bit sequences are generated from the single spatiotemporal chaotic system. In the stream cipher [15], multiple key streams are generated from the coupled map lattice by using simple algebraic computations, and then used to encrypt plain-bits by bitwise XOR. In this paper, we construct a cipher based on hyper- chaos system, and use it to encrypt only some sensitive parameters during video compression, and used a image key for encryption. Compared to the existing ciphers, the proposed cipher considers three aspects, i.e., a lattice initialization method based on iterated Logistic map is proposed to obtain high key sensitivity, the lattice iteration and sequence quantization methods are proposed to generate random sequences and extract the final values of an image key and thus provide security, and the feedback based bitwise XOR is used to encrypt the plaintext. The main advantages of this scheme is that it gives choice data for encryption from an external data or image key, and reduces discover and access to data by attackers.

The rest of the paper is arranged as follows. In Section 2, the cipher based on hyper- chaos system is presented in detail. Then, the video encryption scheme is constructed on the proposed cipher in Section 3. In Section 4, the performances, including security and compression efficiency, are evaluated. Finally, some conclusions are drawn and future work is presented in Section 5.

2. The Cipher Based on Hyper-Chaos System

Encoder structure used in this article is shown in Figure 1. According to this figure, encryption process so that the compressed data for encryption as the DCT coefficients per 8 × 8 block as the primary data send to encoder data [16-18] and this encoder whit support the hyper-chaos functions and using image key, encrypt data [19,20].

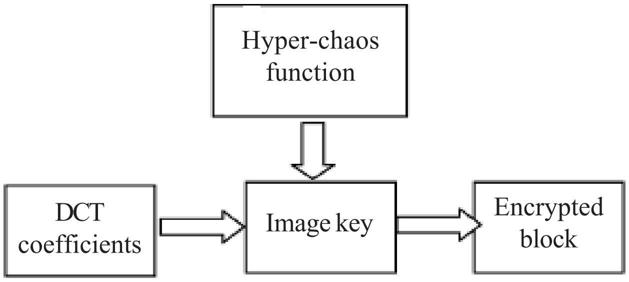

Figure 1. Purposed cipher

2.1 Hyper- Chaos System

Since the vide data to be encrypted are first compressed, the data in block format are provided for encryption. In this case the size of each block is 8×8, thus size of network is same of block. For each 8 × 8 network model is defined as follows:

$$\begin{cases} x_{1,n}^{i,j}1=\pi\left(x_{1,n}^{i,j}+x_{2,n}^{i,j}\right) \\ x_{2,n}^{i,j}1=\pi\left(\cos\left(\left(x_{1,n}^{i,j}+x_{2,n}^{i,j}\right)\times x_{3,n}^{i,j}\right)\right) \\ x_{3,n}^{i,j}1=\pi\left(\cos\left(x_{2,n}^{i,j}+x_{3,n}^{i,j}\right)\right) \\ x_{2,n}^{i,j}1=\pi\left(\sin\left(\left(x_{4,n}^{i,j}+x_{3,n}^{i,j}\right)\times x_{2,n}^{i,j}\right)\right) \end{cases} \quad (1)$$

Four numbers x1, x2, x3, and x4 are as output of hyper-chaos functions after m-iteration for each network. These numbers are real numbers. So that the initial values $0 \leq xl, n \leq 1$ so that $l = 1,2,3,4$ and i, j, respectively number of row and column of each network and are the time points indicated. Therefore we produce number 64 pseudorandom for each 8×8 network.

$$\begin{cases} p_{1,n}^{i,j} = \text{ceil}\left(\text{mod}\left(x_{1,n}^{i,j} \times 10^4, R\right)\right) \\ p_{2,n}^{i,j} = \text{ceil}\left(\text{mod}\left(x_{2,n}^{i,j} \times 10^4, L\right)\right) \\ p_{2,n}^{i,j} = \text{ceil}\left(\text{mod}\left(x_{3,n}^{i,j} \times 10^4, R\right)\right) \\ p_{4,n}^{i,j} = \text{ceil}\left(\text{mod}\left(x_{4,n}^{i,j} \times 10^4, L\right)\right) \end{cases} \tag{2}$$

Four numbers p1, p2, p3, and p4 are used as output functions [19]. R and L indicate the number of rows and the number of columns is this image, respectively. So that the values $1\leq$ P1, n, P3, n $\leq$ R, and $1\leq$ P2, n, P4, n $\leq$ L are located. Finally by combining two of these four values Pi,n so that i =1,2,3,4, we can access and select the pixel in the image. For example, two pixels (P3,P4) and (P1,P2) can be used to specify the address in the image key, and Since image key is a color image and each pixel has three values red , blue and green. Then we used from the output of these hyper-chaos functions to determine and select one of three values for each pixel for the encryption operation, this can be done by the following functions:

$$\begin{cases} y_{1,n} = \text{ceil}\left(\text{mod}\left(\left(x_{1,n}^{i,j} + x_{2,n}^{i,j}\right) \times 10^4, 3\right)\right) \\ y_{2,n} = \text{ceil}\left(\text{mod}\left(\left(x_{2,n}^{i,j} + x_{4,n}^{i,j}\right) \times 10^4, 3\right)\right) \\ y_{2,n} = \text{ceil}\left(\text{mod}\left(\left(x_{1,n}^{i,j} + x_{2,n}^{i,j} + x_{2,n}^{i,j} + x_{4,n}^{i,j}\right) \times 10^4, 8\right)\right) \end{cases} \tag{3}$$

values three $y_{i,\ n}$ (i=1,2,3), according to the equation are set up, but the application of any values according to the encoder performance and initial data cited for the encryption is thus , since each block of 8 × 8 We have a coefficient DC and the rest coefficients AC and in block encryption, only the DC coefficient and the signs of AC coefficients are encrypted in order to reduce the effect on compression efficiency. therefore to encrypt DC coefficient, using of a pixel that is positioned by the P_i, and set of three pages red, blue and green, which determine the page values of $y_{1,n}$, which includes one of values 1, 2 and 3. But to encrypt signs of AC coefficients, the pixels positioning in the image key is set by $P_{i,\ n}$, and using $y_{2,\ n}$ to determine the desired page, then obtain the binary equivalent from value of desired pixel and according to the value $y_{3,\ n}$, bit of pixel select to encrypt the AC coefficients. The operator used, for encryption all coefficients is bitwise operation XOR.

3. Video Encryption Based on the Proposed Cipher

Since video data contain some redundancy. they are often compressed in order to save the space cost of storage or transmission. MPEG2 is typical compression standards for videos.

In MPEG2, the still image is partitioned into 8×8 blocks, and each block is transformed by 8 · 8 DCT, quantized by certain steps, scanned in zig–zag order and then encoded with variable length coding (VLC). Considering that each block is in 8 · 8 size, which is similar with a lattice. Therefore, we use the proposed cipher based on hyper- chaos to encrypt the blocks one by one.

The proposed encryption/decryption scheme is shown in Figure 2. In compression, after color space transformation or block partitioning), DCT transformation and quantization, and the blocks are then post-encoded (i.e., zig–zag scan and VLC) , then the blocks are encrypted by the proposed cipher one by one,. In decompression, the encrypted and compressed media data are firstly decrypted, post-decoded, inversely quantized and transformed, and finally color space transformation or block combining. The decryption process is symmetric to the encryption process.

In block encryption, only the DC coefficient and the signs of AC coefficients are encrypted in order to reduce the effect on compression efficiency. The process shown in Figure 3 is described as follows. Firstly, from the nth block, the parameter set $A_n = a_n^{0,0}, a_n^{0,1}, ..., a_n^{7,7}$ is extracted. Here, $a_n^{0,0}$ is the DC, while the others are the sign-bits of the ACs, respectively. If the i, j th AC is bigger than 0, then $a_n^{i,j} = 1$. Otherwise $a_n^{i,j}$ =0.

Secondly, the extracted parameter set is encrypted by the chaotic lattice according to the method proposed in Section II. Then, the encryption operation for DC coefficient is defined as:

$$C_n^{0,0} = a_n^{0,0} \oplus image\_key\left(p_{1,n}^{0,0}, p_{2,n}^{0,0}, y_{1,n} \right) \tag{4}$$

In accordance with the above equation set of key pixels image DC coefficients by bit XOR operator encrypted.. But for the rest of the coefficients, including AC coefficients, according to the encryption algorithm and to increase our rate, the signs of these coefficients are encode, for this purpose, performing the following:

First, according to equation 5, determine selected pixels of image. Then, using equation 6 with the help of hyper- chaos functions, variable $y_{3,n}$ determines the bits selected from the pixels selected for encryption, We repeat work for all coefficients in all time periods.

$$\begin{cases} pixel\_sel_n^{i,j} = image\_key\left(p_{3,n}^{i,j}, p_{4,n}^{i,j}, y_{2,n} \right) \\ \left(i, j = 0,1,\ldots,7 \text{ and } i = j \neq 0, n = 0,1,\ldots, N-1 \right) \end{cases} \tag{5}$$

$$\begin{cases} bit_{sel_n^{i,j}} = pixel_{sel_n^{i,j}} \left(y_{3,n} \right) \\ \left(i, j = 0,1,\ldots,7 \text{ and } i = j \neq 0, n = 0,1,\ldots, N-1 \right) \end{cases} \tag{6}$$

$$\begin{cases} c_n^{i,j} = a_n^{i,j} \oplus bit_{sel_n^{i,j}} \\ \left(i, j = 0,1,\ldots,7 \text{ and } i = j \neq 0, n = 0,1,\ldots, N-1 \right) \end{cases} \tag{7}$$

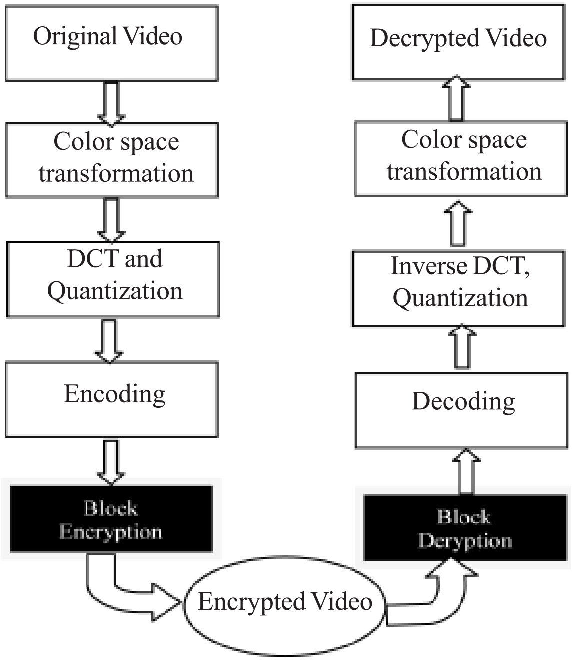

Figure 2. Architecture of the Encryption/Decryption Scheme

4. Performance Evaluation

A good encryption should resist all kinds of known attacks, it should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible.

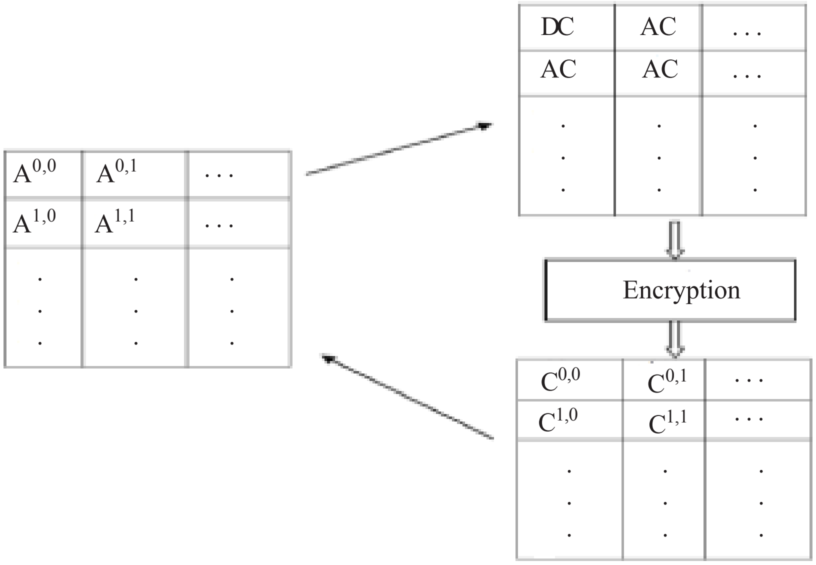

Figure 3. Block encryption

4.1 Key Space Analysis

Since the encryption key in different two-step producted and is used, Furthermore, the complexity of the algorithm raised, and it is indistinguishable, a key in the first step as input hyper- chaos functions is a 32-bit key, and space as large as the 232, but the image key in the next step to perform encryption is used, a picture with size N × M, which was three pages, in total our key space is as big as 224×N×M will. So increase of the key space result higher security.

4.2 Randomness and Key Sensitivity of the Produced Sequences

It can be said about randomness that under the above conditions and using these complex chaos functions, pseudorandom sequences, with high levels randomness are produced. So it can be concluded that hyper-chaos encryption algorithm is sensitive to the key. small change of the key will generate a completely different decryption result and cannot get the correct plaintext. Randomness of hyper-choas functions is shown in figure 4.

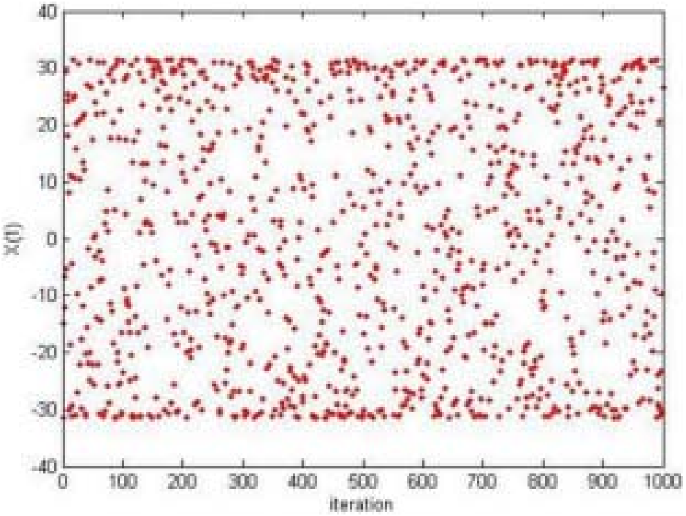

Figure 4. Randomness of hyper-choas functions

4.3 Security of the image/video encryption scheme

Different video applications require different levels of security. For multimedia encryption, besides the security of the cipher, the perceptual security should also be confirmed. In this section, based on the implementation of the proposed method on video data, including Salesman, Akiyo, Foreman, Stefan with specific frame number and size, pay to evaluate the results. Encryption results are presented in Figure 5. To measure the quality of the encrypted content, the peak signal-to-noise ratio (PSNR) is tested. PSNR was calculated for vidoes presented in Table I.

Videos	**PSNR(db)**		
	y component	**u component**	**Yuvcomponent**
Stefan	13.4369	12.1670	9.9660
Foreman	11.5638	11.0838	10.4427
Akiyo	16.4143	13.2990	11.3551
Salesman	17.5727	13.8912	11.7581

Table 1. PSNR Values of Different Video Sequences

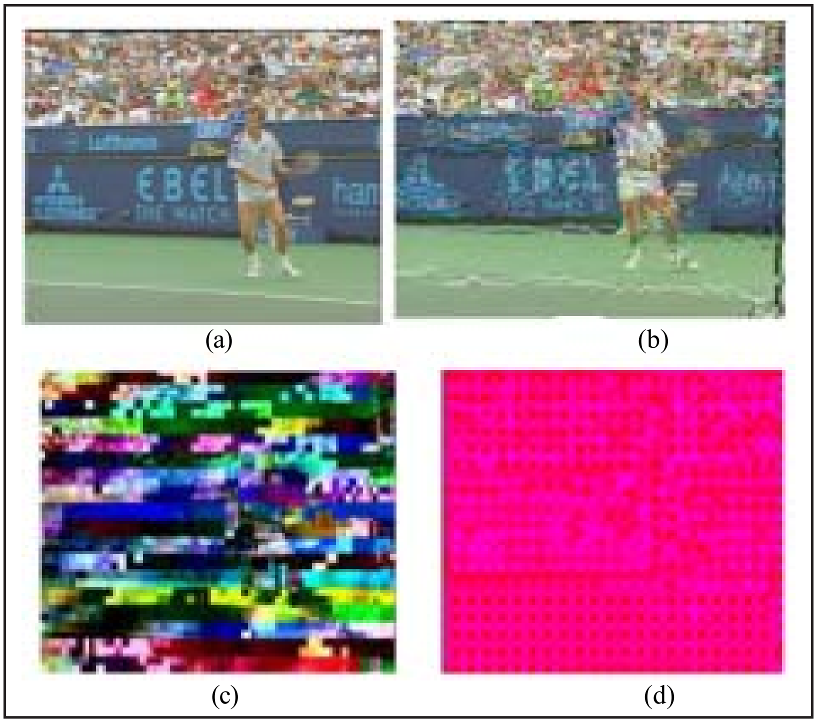

Figure 5. Results of video encryption. (a) original video,(b) encrypted by AC sings, encrypted by DC, (d) encrypted by DC+AC sings

4.4 Compression efficiency

Video compression and encryption are associated processes in secure multimedia systems and applications. A video encryption algorithm should not cause impairment on the compression efficiency, i.e. the size of the compressed video stream should not be increased by the encryption. Firstly, the proposed scheme changes only the DC and signs of AC, which changes the compression ratio slightly. According to MPEG2 [21], the changes of AC s signs do not change compression ratio, while the changes of DC change the VLC length of DCs. Thus, for video encryption, the computational cost is very little compared to video compression, which is suitable for real-time applications. Additionally, taking various videos for example, the time ratio between encryption operation and compression operations are tested and shown in Table 2. It show that the encryption operation is time efficient compared to compression operations.

Videos	Time ratio (%)	
	Encryption/compression	Decryption/decompression
Stefan	1.1	2.3
Foreman	0.95	1.9
Akiyo	1.0	2.1
Salesman	1.5	3.7

Table 2. Test of Time-Efficiency

5. Conclusions and Future Work

In this paper, a scheme for video encryption are presented, which is based on hyper-chaos system and uses a imge key for the high-security encryption. Beginning a stream cipher is constructed based on the pseudorandom sequences generated by the Hyper-chaos lattices. Then the selected pixel and bitpixel of image key encrypt frame blocks one by one. By iterating chaotic maps for certain times, the generated pseudorandom sequences obtain high initial-value sensitivity and good randomness. The pseudorandom-bits in each lattice are used to select pixel and bitpixel of image key and then encrypt the Direct Current coefficient (DC) and the signs of the Alternating Current coefficients (ACs). The main feature of our scheme is using of image key, that increase key space and complexity, thus encryption security rises. The scheme s performances are tested and analyzed, which include the security of the stream cipher, the perceptual security of the encrypted videos, and the effect on compression efficiency (compression ratio and computational cost). The results show that the proposed stream cipher satisfies the requirement of secure encryption principles, the encrypted videos are secure in perception, the encryption operation does not change the compression ratio apparently.

References

[1] Gonzales, O., Han, G. , Gyvez, J. and Sanchez-Sinencio, E. (2000). Lorenz-based chaotic cryptosystem: a monolithic implementation, *IEEE Trans Circuits Syst*. I, V. 47, p. 1243–1247, Aug.

[2] Mollin, RA. (2006). An introduction to Cryptography. 2nd ed. CRC Press.

[3] Dedieu, H., Kennedy MP., Hasler, M. (1993). Chaos shift keying: modulation and demodulation of a chaotic carrier using selfsynchronizing Chua s circuits, *IEEE Trans Circuits Syst* II, 40 (October):634–42.

[4] Short, KM. (1994). Steps toward unmasking secure communications, *Int J Bifurcat Chaos*, 4 (4) 959–77.

[5] Goetz, M., Kelber, K., Schwarz, W. (1997). Discrete-time chaotic encryption systems – Part I: Statistical design approach. *IEEE Trans Circuits Syst* I, 44 (October) 963–70.

[6] Dachselt, F., Kelber, K., Schwarz, W. (1998). Discrete-time chaotic encryption systems – Part III: Cryptographical analysis. *IEEE Trans Circuits Syst* I, 45 (September):983–8.

[7] Lian, S., Sun, J., Wang, J., Wang, Z. (2007). A Chaotic Stream Cipher and the usage in Video Protection, *Chaos, Solitons & Images,* 34 (3) 851–9.

[8] Frey, DR. (1993). Chaotic digital encoding: an approach to secure communication. *IEEE Trans Circuits Syst*II, 40 (October) 660–6.

[9] Tsueike, M., Ueta, T., Nishio, Y. (1996). An application of two-dimensional chaos cryptosystem, Tech Rep IEICE, NLP96-19, May.

[10] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurcat Chaos*, 8 (6) 1259–84.

[11] Chen, G., Mao, YB., Chui, CK. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, *Solitons & Images*, 12. 749–61.

[12] Zhou, Q., Wong, K., Liao, X., Xiang, T., Hu, Y. (2008). Parallel image encryption algorithm based on discretized chaotic map. Chaos, *Solitons & Images* 2008, 38 (4) 1081–92.

[13] Gao, T., Chen, Z. (2008). Image encryption based on a new total shuffling algorithm, *Chaos, Solitons & Images*, 38 (1) 213–20.

[14] Zhang, L, Liao, X, Wang, X. (2005). An image encryption approach based on chaotic maps. *Chaos, Solitons & Images*, 24 (3) 759–65.

[15] Li, P., Li, Z., Halang, WA, Chen, G. (2007). A stream cipher based on a spatiotemporal chaotic system. *Chaos, Solitons & Images*, 32 (5) 1867–76.

[16] Li, Y, Cai, M. (2009). H.264-Based Multiple Security Levels Net Video Encryption Scheme, *IEEE Trans. on Electronic Computer Technology.*

[17] Liang, S. (2009). Efficient image or video encryption based on spatiotemporal Chaos system. *Chaos, Solitons & Images* 40, 2509–2519.

[18] Yang, S., Sun, S. (2008). A video encryption method based on chaotic maps in DCT domain. *Progress in Natural Science* 18, 1299–1304.

[19] Valerij, R. (2009). Modulo image encryption with image keys . *Optics and Lasers in Engineering* 47, 1–6.

[20] Gao, T., Chen, (2008). A new image encryption algorithm based on hyper-Chaos, *Physics Letters* A 372, 394–400.