Video encoding by using cellular automata based on chaos theory

Saeed teimoori
Department of computer science, Faculty of computer science and mathematics,
university of shahid-bahonar, kerman, iran
saeed.teimoori@gmail.com

Reza saravani
Department of information technology, faculty of electrical engeering And computer engeering,
azad islamic university of Rafsanjan, rafsanjan, iran
reza.s@yahoo.com

Abstract - In recent years has arisen high speed in growth of transmission video media. In this paper presented a method for encode video by using the above functions Kayes and cellular automata. In this our method partake from hyper-chaotic functions capabilities which include sensitivity to initial values, pseudo-random and non-periodic behavior is function along with cellular automata capabilities. Due to the complexity in which there is hyper-chaotic function and also been big key space toward to normal chaos functions, There are more resistant versus hacker attacks and consequently significantly increased security. Pseudo-random bits employed in each network for encoding the coefficient of direct current (DC) and alternating current coefficients (AC). The obvious point proposed scheme use of cellular automata are enhance the speed cryptography and therefore improving security. The results show that this scheme has good steganography security and perceptual and complexity speed, also there are not effect on compression efficiency that this method has made efficient and effective.

Key Words: Security, video encoding, hyper-chaotic, cellular automata.

1. Instruction

Advantages of chaos theory for data protection purposes are now obvious. In addition, the characteristics of sensitivity to initial value and sensitivity to initial parameters, these values and parameters perfect pick up for use as an encryption key. So far, some of the data protection tools have been proposed, data encryption is also typical of them. Data encryption [1] often the initial data converted into a form that to be protected from them confidential. Only authorized users has access to the correct key successful recovery of data. Many algorithms have been reported based on numerous chaoses. Algorithms are classified into several types based on characteristics that include: chaos switching, chaos modeling, chaos current code, chaos block code and other types are encryption algorithms. In chaos switching [2] chaos two systems is used to represent 0 and 1 signals. In chaos modeling [3] chaotic sequence is used as a carrier of messages, Thus in the time to send chaos sequence added to the message and the sequence produced is sent. At the time receiving are low chaos sequence and the message is retrieved. In chaos current code caused a current key by chaos sequence manufacturer and to encrypt the initial text is used as one-to-one. For example, some of code systems based on chaos message are by chaotic signals generated from time continuous chaos dynamical systems [4], Discrete chaos dynamical systems [5,6] or tightly coiled networks modeling [7]. Chaos block code original text transmits as block to block and by mapping the chaos. For example, the encoder is structured based on the modified design [Baker 8], discrete two-dimensional design [Baker 9] or chaos three-dimensional designs [10]. Due to simply chaos in the implementation being used this theory for image or video encoding which are often with high volumes of data. For example, Kolmogorov design is used order to design parallel image encryption algorithm [11], the two chaos mapping are combined for the mixing of image pixels [12], Non-linear algorithms have been introduced to image encryption linear function replace [13], chaos characteristics and spread exponential chaos mappings to be improved and for encryption algorithms being used [14], Bakar design allows to encoder structuring an image block [8]. This image coding encoded to directly and without compression. Virtually image or video to save in storage space and communication load, are compressed. So it is reasonable to before data from encrypt, we compressed. So with consider this fact that an image and video has high data volumes, compressed data encryption and reduces the time cost. However, data volumes are high and timing. So as to reduce time, we just code parts certain of the compressed data. Chaotic system structure desired according the type of data is space and time. Space chaotic system being used in both of current encoders and the block encoders. Because we have need to access data in different places and schedules, to solve the problem, takes the place of chaos function that producing different amounts at different times. Thus partake from tightly coiled a network, which generates pseudo-random values, these networks have good hiding characteristics. In the current encoders are produced [15] multiple the current key from tightly coiled networks by using simple algebraic calculations, and encoded

by the operator initial data XOR bit. Another issue that needs to be considered in the discussion is high security encryption.

In this paper, we partakes encoder based on hyper-chaos function, which are spatial when acts, with these difference that for the encoding using from a two-dimensional cellular automata. Compared with other things we are considering to several aspects: Initialize the network, repeat in the networks and extracting the final values network from an image provides randomization and therefore security, XOR Bit operator being used order to encode the data. In the proposed method are encrypted video data as block blocks, As a result, the size of any the network to choice block size was video and is fixed. Values depend on in the tightly coiled networks and values in networks n-th to value before network it.

The remaining contents of this paper are as follows: In section 2 are review encryption systems based on cellular automata and hyper-chaos system of the proposed to detail. Then, in Section 3 encryption design based on the proposed encryption is structured. In Section 4, the proposed method includes security; compression efficiency and speed are evaluated. Finally, Section 5 Conclusions and future works will be discussed.

2. Encryption based on hyper-chaotic systems and cellular automata

The encoder general framework of the overall structure of the encoder used in this paper is shown in Figure 1. According to this encryption process so that compressed data for the encoding as DCT coefficients in each block 8×8 given as the initial data is to encrypt the data [16-18] and it encrypts to help hyper-chaotic functions and by using of cellular automata [19] two-dimensional is encrypted.

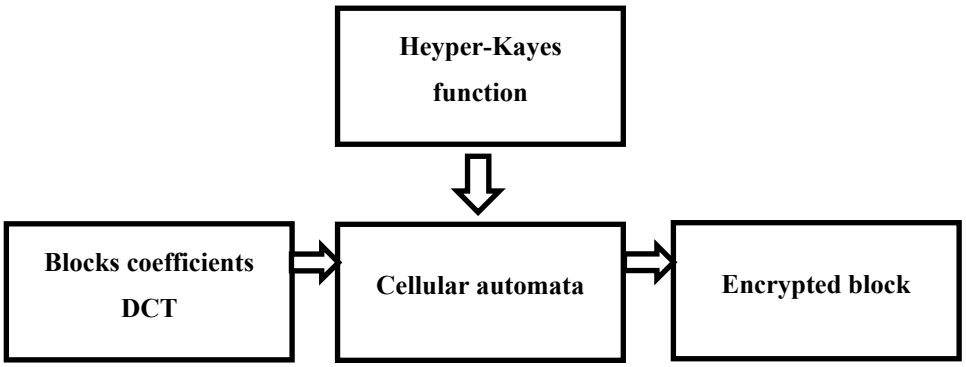

Figure 1: encryption based on cellular automata

2.1. Cellular Automata

A cellular automaton was introduced in 1940 by von Neumann. Cellular Automata are dynamic systems in terms of time, place and discrete states. Cellular automata includes an array of cells that each cell has a value of possible states which all cells simultaneously in discrete time steps are updated in accordance with the special law. [19,20] State of the cell can be any integer number. Neighbors cells are included self-cells and neighboring cells it. Cellular automata in action can be one, two, or three dimensions. In automata the one dimension, a local neighbor cells connected to r (r is the radius of the law). [20,21] The simplest Cellular automata has a radius of 1 and two states (0.1). Conclusion functions or law development of f simple Cellular automata as follows:

$$S_i(t+1) = f(s_{i-1}(t) \text{ ، } S_i(t) \text{ ، } s_{i+1}(t)) \quad (1)$$

Which s is state cellular automata, S_i (t) expresses cell state i at the time t [22].

Because of its algorithm and implementation simple hardware is of particular importance in the production of pseudo random number. In this method, a set of cells grouped, each cell with neighboring cells have a cellular automaton, its value is defined by law. [22] Since performance can not easily be guessed from its cellular automata in the next step are used to generate pseudo random numbers. The problem this method produced a short sequence of numbers so that series of numbers generated repeatedly. To solve this problem have been proposed synthetic laws or compound automatically that has considerable improves generate random numbers situation but problem its the use of several laws and thus more complex hardware. Also because the simplicity of the performance of automaton, decrypt the information is easy.

2.2. Hyper-chaotic systems

Since video data order to encrypt beginning to compresses, these data are provided for the encoding in the form of blogs. The size of each block is 8×8, As a result, so is the size of the network. For each network 8 × 8 model is defined as follows:

$$x_{1,n}^{i,j} = \pi(x_{1,n}^{i,j} + x_{2,n}^{i,j})$$
$$x_{2,n}^{i,j} = \pi(\cos((x_{1,n}^{i,j} + x_{2,n}^{i,j}) \times x_{3,n}^{i,j}))$$
$$x_{3,n}^{i,j} = \pi(\cos(x_{2,n}^{i,j} \times x_{3,n}^{i,j}))$$
$$x_{4,n}^{i,j} = \pi(\sin(x_{3,n}^{i,j} \times x_{4,n}^{i,j}) + x_{2,n}^{i,j})$$

The four numbers X_1, X_2, X_3, X_4 are as output functions hyper-Kayes top after m iterations for each area of the image. These numbers are real numbers. So that the initial values $-\pi \leq x_{4,n} \leq \pi$ and i, j respectively represent the row and column each network and n represents the point time. Amount of X_4 by hyper-chaos functions from the previous step obtained to initialize used for Cellular automata.

3. Video encoding based on the proposed encryption

Since multimedia data are image and video has redundancy, most of these data compression to reduce storage space and transfer. For those who been agree with communications hidden algorithms that are associated with compression, we examined. JPEG and MPEG 2 standard for image and video are two types of compression devices. In both of them still image is divided into 8×8 blocks, and each block has been transferred by 8×8 DCT, by determination steps digitized in a zigzag practices gets scrolling and then with a variable length coding (VLC) is encrypted. Since block size is the same with network, we recommend encryption based on irregularities for hidden one to one blocks. The structure of algorithm encryption / decryption suggested shown in Figure 2.

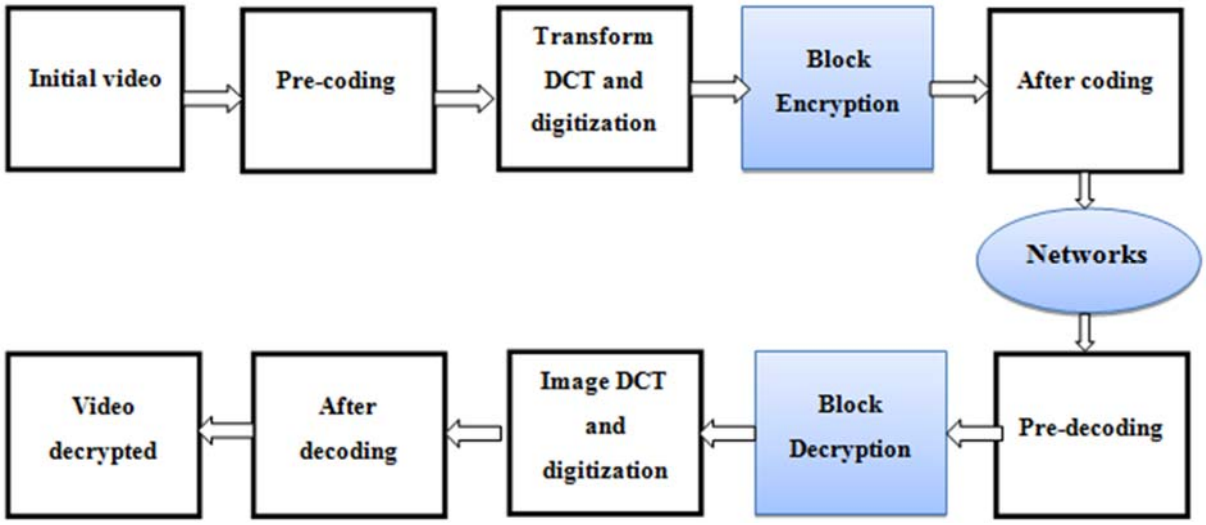

Figure 2: Structure encrypt / decrypt video with the proposed method

In compression after the initial encryption (color space conversion and segmentation blocks) [16], conversion DCT and digitization blocks by encryption proposed are hidden, and block is encrypted then spent the final hidden (Zigzag scrolling and VLC). In image compression data is compressed and encrypted before first decoding, then decoding operation, photos digitization taken conversion and finally decoding done. Decoding action is symmetric with encryption operation. In the encryption block, only DC coefficient and AC coefficient symbols are encrypted to reduce the impact on the compression efficiency. This process is shown in Figure 3 is as follows: First, the n-th block, set parameters $A_n = a_n^{0,0} a_n^{0,1} \ldots a_n^{7,7}$ are extracted. Here, $a_n^{0,0}$ equal DC coefficient and the remaining bits are AC symbols. If i,j-th AC is greater than 0, $a_n^{i,j} = 1$ otherwise is $a_n^{i,j} = 0$. Second, the parameters extracted by irregularities network and are encryption in the following. For the DC coefficient included in each block with the following equation:

$$C_n^{0,0} = a_n^{0,0} \oplus cells_n^{0,0}$$

Determined in accordance with the above equation bits from cellular automata with DC network coefficient by XOR bit operator is encrypted. But for the remainders of coefficients which include were AC coefficients and accordance with algorithm to increase the speed of encryption will encrypt symptoms of these coefficients.

$$C_n^{i,j} = a_n^{i,j} \oplus cells_n^{i,j}$$

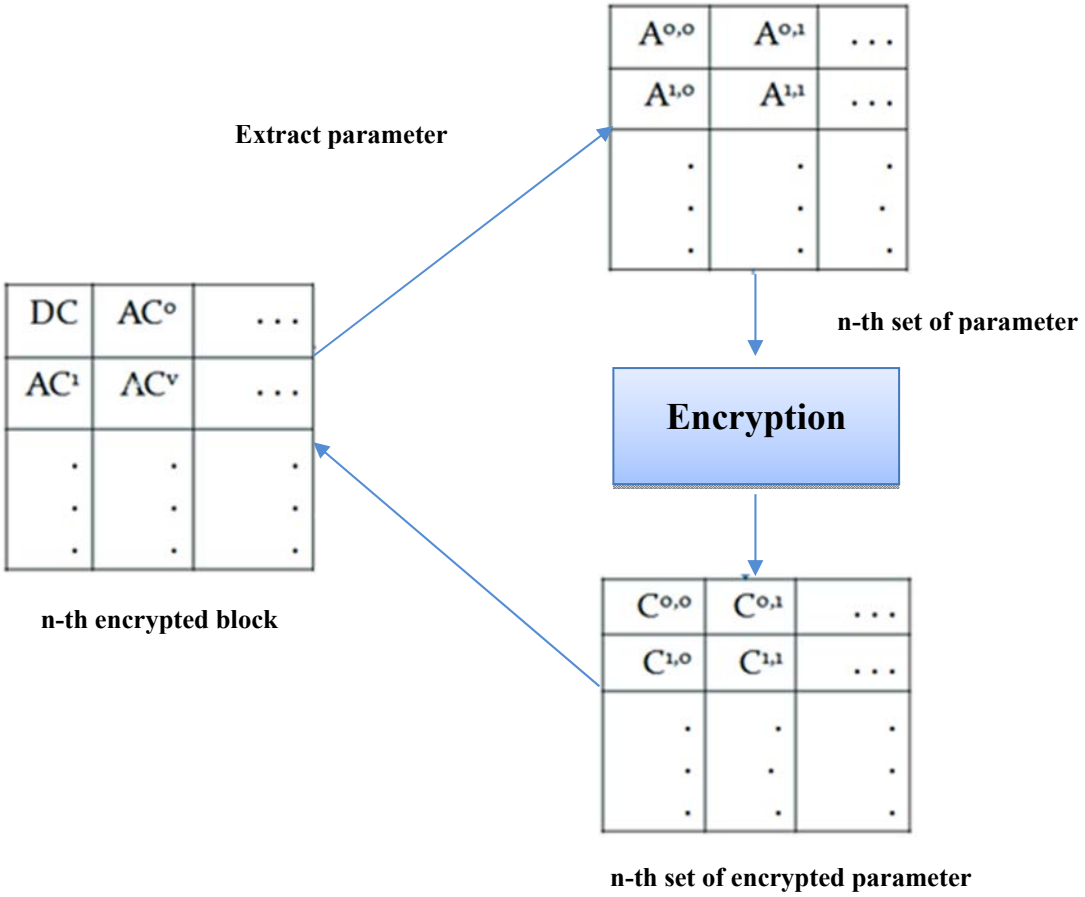

Figure 3: block encryption process

4. Video decoding

Decoding is symmetric with encryption. In decoding data compressed and encrypted the first pre-decoding, then taken act of decoding, digitization photos and conversion and finally done post-decoding.

In the decoding block, only the DC coefficient and AC coefficient are decoding symbols. This process is as follows: First, from nth block $C_n = c_n^{0,0} c_n^{0,1} \dots c_n^{7,7}$ set parameters are extracted. Here $C_n^{0,0}$ equal the DC coefficient and the remaining AC symbols bits are encrypted. If i,j th AC is greater than 0, $C_n^{i,j} = 1$ in the otherwise is $C_n^{i,j} = 0$. Second, parameters obtained by irregularities network and are decoding as the following.

$$a_n^{i,j} = C_n^{i,j} \oplus cells_n^{i,j}$$

5. Performance evaluation and simulation results encryption

In this section several simulation examination of the proposed system properties on the video data included Salesman, Akiyo, Foreman, Stefan was conducted with numbers frame rate and size specified. The simulation was performed by MATLAB software.

5.1. Theoretical study security in proposed encryption

In the proposed encryption, pseudo-random sequences generated by the system and function hyperchaotic and the original are used for data encryption. In such systems security to key space and randomization depends on a pseudo-random sequence. These issues accordance with analysis and review thus are available.

5.2. Key space in suggested encryption

Key size used in this method is as follows: 4 bits to store the initial value of hyper-chaos functions, 8 bytes to store the number of occurrences the mapping of chaos for initializing to cellular automata (One byte for every row), A bit to save the number of repetitions to update cellular automata. Therefore, key size is 13 bytes. Or in other words, 2104 will be the space key. We will achieve greater security by increasing the space key.

5.3. Histogram analysis

The number of pixels per gray level for an image shows histogram. In general, what is more uniform image histogram obtained suggest the possibility of attacks on its statistical will be less.

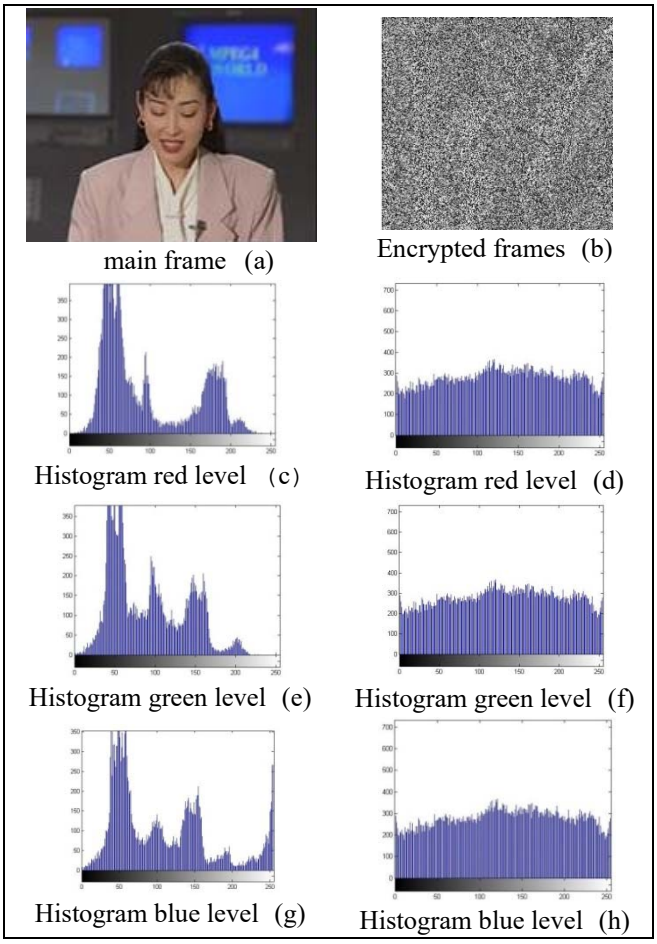

Figure 4: The Figure a is selection frame from the original video and figure b is encrypted frame. Figures are specified c and e, and g, respectively histogram of the red, green and blue original frame and d and f and h respectively histogram figures of red, green and blue levels in the frame. As images d, f and h can be seen, the encrypted image histogram is uniform and the possibility of attacks on its statistical will be less.

5.4. Randomization and sensitivity to key in created sequences

In the case of randomization can be said that under the conditions mentioned and using hyper-chaos complex functions and cellular automata, pseudo-random sequences can be created to top randomization. Also encryption algorithms from hyper-chaos functions that take advantage to create chaotic sequences, Key to the initial value are sensitive and the slightest change in the initial value key led to the creation sequence gets completely different. Figure 5 shows the sequence distribution produced by the variable shown X_4, which represents randomization hyper-chaos functions.

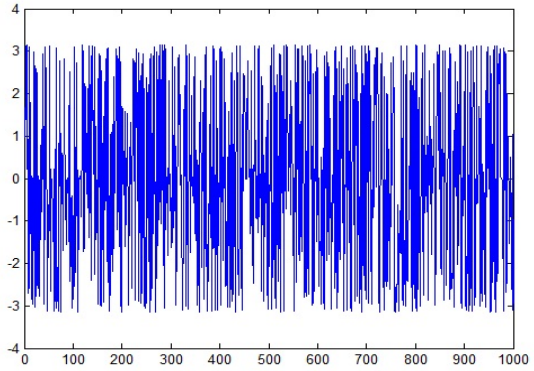

Figure 5: randomization in hyper-chaos function for variable

5.5. Amount security in video encoding scheme

Since in the proposed scheme DC coefficient and AC coefficient signals are encrypted and energy had been low frequency coefficients, encryption DC coefficient reduces quality, In case encryption signals AC coefficients lead to increased energy loss. In this section based on the implementation of the proposed method on the video data includes stefan, foreman, Akiyo, Salesman pays to frame numbers and Sizes specified to examine results. Encryption results are shown in Figure 6. For this purpose, we use the concept of PSNR to evaluate the encoder quality. First, we determine the amount of MSE between the primary video and the video is encrypted by the equation.

$$MSE = \frac{1}{3 \times m \times n} \sum_{Y,U,V} \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} \left(E(j,k) - D(j,k)\right)^2$$

M and n in the above equation video frame size E (j, k) the amount of pixels in the initial video and D (j, k) the amount of pixels in the video is encrypted. Then to help the following equation obtains PSNR value between Initial video with the encrypted video.

$$PSNR = 10 \log_{10}\left(\frac{MAX^2}{MSE}\right)$$

Table 1: PSNR related to video data

PSNR	Initial video
36.3	Stefan(176×144)
36.1	Foreman(176×144)
35.4	Akiyo(176×144)
38.2	Salesman(176×144)

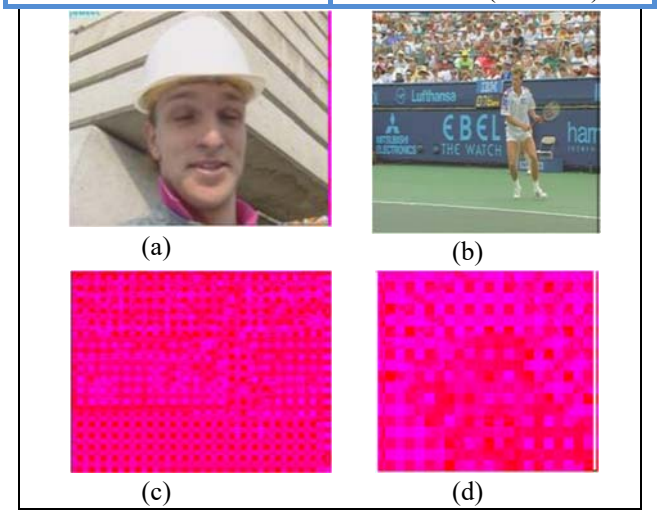

Figure 6: video before and after encryption: (a) stefan, (b) foreman, (c) stefan after encryption, (d) foreman after encryption

5.6. Compression efficiency

In the proposed scheme encryption operations have been combined with compression and image compression process. Given the choice data to encrypt, it seems that there is no much impact on compression efficiency because in proposed scheme only DC coefficients signals and AC coefficients are encrypted and changes very low ratio compression. Based on the structure MPEG change in signals AC compression has not made any change in the ratio, while changing in DC the length of VLC coefficients DC changes. But the same type select data order to encryption also reduces the time required for encryption, So that the time required for encoding to compress time is very small. The result in Table 2 on experimental data shows the truth of this matter.

Table 2. Ratio of time encryption to compression

Ratio of time encryption to compression	Initial video
0.011	Stefan(176×144)
0.009	Foreman(176×144)
0.010	Akiyo(176×144)
0.015	Salesman(176×144)

6. Conclusion and Suggestions

In this paper, a method is provided for video encoding. The proposed scheme were based on hyper-chaos and cellular automata functions and has a complex key is used for securing high. Results of experiments performed indicate the fact that the proposed scheme has high security hidden, also does not effect on performance Compression. These characteristics proposal scheme as to converts an appropriate method for applications. As future works can also be the proposed scheme with an image, or a video frame combine to increase system security.

Reference

[1] Gonzales O, Han G, Gyvez J, and Sanchez-Sinencio E(2000). 'Lorenz-based chaotic cryptosystem: a monolithic implementation', IEEE Trans Circuits Syst. I, vol. 47, pp. 1243–1247
[2] Mollin RA. An introduction to cryptography. 2nd ed. CRC Press; 2006.
[3] Dedieu, H, Kennedy, MP and Hasler, M.(2002) 'Chaos shift keying: modulation and demodulation of a chaotic carrier using selfsynchronizing Chua's circuits', IEEE Trans Circuits Syst, vol. 40, pp. 634–642
[4] Short, KM.(1994)'Steps toward unmasking secure communications', International Journal of Bifurcation and Chaos, Vol. 4 No. 4, pp.959–977
[5] Goetz, M, Kelber, K, and Schwarz, W. (1997) 'Discrete-time chaotic encryption systems – Part I: Statistical design approach',IEEE Trans Circuits Syst, Vol. 25 No. 10, pp.963–970
[6] Dachselt, F, Kelber, K and Schwarz, W. (1998) 'Discrete-time chaotic encryption systems – Part III: Cryptographical analysis',IEEE Trans Circuits Syst, Vol. 45 No. 9, pp.983-988
[7] Lian, S, Sun, J, Wang, J and Wang, Z. (2007) 'A chaotic stream cipher and the usage in video protection', Chaos, Solitons & Fractals, Vol. 39 No. 3, pp.851–859
[8] Frey, D.R. (1993) 'Chaotic digital encoding: an approach to secure communication', IEEE Trans Circuits Syst, Vol. 40 No. 10, pp.660-666
[9] Tsueike, M, Ueta, T and Nishio, Y. (2011) 'An application of two-dimensional chaos cryptosystem', Tech Rep IEICE, NLP96-19, May 1996.
[10] Fridrich, J. (1998) 'Symmetric ciphers based on two-dimensional chaotic maps', International Journal of Bifurcation and Chaos, Vol. 8 No. 6, pp.1259-1284
[11] Chen, G, Mao, YB and Chui, CK. (2004) 'A symmetric image encryption scheme based on 3D chaotic cat maps', Chaos, Solutions & Fractals, Vol. 21 No. 3, pp.749–761
[12] Zhou, Q, Wong, K, Liao, X, Xiang, T and Hu, Y. (2008) 'Parallel image encryption algorithm based on discretized chaotic map', Chaos, Solutions & Fractals, Vol. 38 No. 4, pp.1081–1092
[13] Gao, T and Chen, Z. (2008) 'Image encryption based on a new total shuffling algorithm', Chaos, Solitons & Fractals, Vol. 38 No. 1, pp.213–220
[14] Zhang, L, Liao, X and Wang, X. (2005) 'An image encryption approach based on chaotic maps', Chaos, Solitons & Fractals, Vol. 24 No. 3, pp.759–765
[15] Li, P, Li, Z, Halang, WA and Chen, G. (2007) 'A stream cipher based on a spatiotemporal chaotic system', Chaos, Solitons & Fractals, Vol. 32 No. 5, pp.1867–1876
[16] Li Y,Cai M. H.264-Based Multiple Security Levels Net Video Encryption Scheme, IEEE Trans. on Electronic Computer Technology, (2009).
[17] Liang, S. (2009) 'Efficient image or video encryption based on spatiotemporal Chaos system', Chaos, Solitons & Fractals, Vol. 40 No. 5, pp.2509–2519
[18] Yang, S and Sun, S. (2008) 'A video encryption method based on chaotic maps in DCT domain', Progress in Natural Science, Vol. 18 No. 10, pp.1299–1304
[19] Tomassini, M and Perrenoud, M.(2001) 'Cryptography with cellular automata', Applied Soft Computing Journal, Vol. 1, pp.151-160
[20] Xuelong, Z, Qianmu, L, Manwu, X and Fengyu, L.(2005) 'A Symmetric Cryptography Based On Extended Cellular Automata', IEEE International Conference, Vol. 1 , pp.499-503
[21] S. Wolfram, A New Kind of Science. Illinois:Wolfram Media, Inc., 2002.
[22] S. Wolfram, Cryptography with Cellular automata, in:Advances in Cryptography Crypto 85 Proceeding, LNCS 218, Springer, 1986,pp 429-432