VIDEO ENCRYPTION BASED ON CHAOTIC SYSTEM AND STREAM CIPHER

Mahmood K. Ibrahem[1], **Laith Abdulhussein Hamood** [2]
[1]College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
[2]Iraqi Commission for Computers and Informatics, informatics institute for postgraduate studies, Baghdad, Iraq
mahmoodkhalel@coie-nahrain.edu.iq[1], laithhamood@gmail.com[2]

Received:22/05/2018, Accepted:30/5/2018

***Abstract*-The huge development and use of digital multimedia (video, image) over computer networks has led to increase the need for securing of these digital data. Video encryption is widely used as a method for providing security for digital video. In this paper video encryption method is developed using chaotic system for key generator and stream cipher, it uses chaotic map as one-time key generator which produce key used for encryption process. Chaotic systems have been successfully used for multimedia encryption. Chaotic cryptography have good characteristic such as pseudo-randomness, and sensitivity to initial conditions. Video encryption method have successfully designed and implemented, the tests and analysis results have showed the succeed of the encryption method in term of speed and security.**

***Keywords:* video encryption, chaotic system, cat map, logistic map**

I. Introduction

The rapid development in multimedia communication and networks technologies lead to huge increase in using and transmitting of digital video data over networks these video data could be a private, commercial or personal data containing sensitive information so should not be reveal into unauthorized users. Video encryption is very useful method to provide protection for video data [1].

Where encryption mean the processes of transforming the original data into a form that cannot be read by unauthorized users in order to provide protection to the data been encrypted [2]. There are many traditional efficient encryption algorithms but most of them not suitable to be used for video encryption directly. In this paper we present effective encryption algorithm in term of speed and security which is based on one-time-pad key stream cipher and chaotic system.

Many researcher devote their research to find out effective method for video encryption [3] proposed method for video encryption based on using logistic map as chaotic sequence to be used as an encryption key where two logistic map are adapted to produce chaotic sequence which used for scrambling of DCT coefficients of the frame and use specific formula to encrypt the scrambling frame. In [4] proposed method they suggest to use cat map and piecewise linear chaotic map together to having fine pseudorandom characteristics. By using these chaotic maps to generate key sequence in order to be used for encryption and to generate permutation list, the whole process is first selected data of each frame is encrypted then perform permutation on the macroblock of each frame to obtain the decrypted video. The inverse operation is used to decrypt the video. [5] Gave a suggestion for video encryption by using discrete piecewise linear map as a chaotic system for chaotic sequence generator and using of stream cipher to encrypt the selected video data. In [6], they used couple of logistic maps to generate sequence of chaotic to get the encrypted video. First, video data is encrypted with first logistic map, the result of this encryption will be encrypted for another time with the second sequence. In [7] the researchers proposed method that use double chaotic maps for sequence generating each map will produce sequence those sequences are combining to each other either by Xoring them or adding depend on if the value of the sequence is the same or different. The obtained sequence will be used for encryption by using formula based on Xoring and addition.

II. Chaotic System

Chaotic system has been established from many different research areas, such as physics, mathematics, which is nonlinear dynamic system that can be presented mathematically through specific formula called chaotic maps. Chaotic maps divided into two types discrete maps and continuous maps, an example of the discrete systems are Logistic map and Arnold cat map. And an example of continues system are The Lorenz system and Rossler system.Chaotic systems have sensitive dependent on initial conditions. If two initial points are chosen very close to each other, the distance between their successive orbits under chaotic map diverges exponentially. Hence, a chaotic system can be used as a pseudo-random number generator [8] and [9]

a- Logistic map:Its one of the simplest maps that present Chaotic behavior, its used in many application and cryptography system that are based on chaotic system [8]. It can be describing in the following mathematical equation: [10]

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

Where x is number ranging from 0 to 1 and x represents the initial value or seed for logistic equation. The μ represent the equation parameter which is a number in the range (3.569946,4)[10].

b- Arnold cat map: Vladimir Arnold is the inventor of Arnold cat map he proposed the cat map as 2D chaotic system. Arnold cat map is discrete chaotic system since of its invention it used in many encryption methods especially for image encryption. Its transformation map mathematically can be describe as following: [11] and [12].

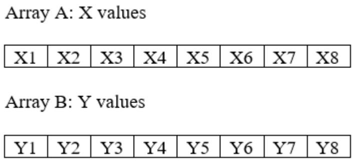
$$x_{n+1} = (2 \cdot x_n + y_n) mod\ 1, \tag{2}$$

$$y_{n+1} = (x_n + y_n) mod\ 1, \tag{3}$$

where x_{n+1}, y_{y+1} are the new points and x, y are the original points.

III. Key Generation Process

Encryption key is an essential part of any encryption method. In this paper chaotic maps are used as key generator. We suggest two approaches to generate key; first approach depend on cat map and the second is used cat map along with logistic map as combination of two chaotic systems to generate the key.



Array A: X values

X1	X2	X3	X4	X5	X6	X7	X8

Array B: Y values

Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8

Figure 1: X,Y values

- ***First approach*** Generating key sequence by depending on the equations of cat map, first initial value between (0,1) for x, y are set iterate the cat maps for a specific number of iterations, each value for each iteration is converted into set of bytes to be inserted into an array of bytes, so there will be two arrays each one holds different values as shown in Fig.1. After inserting all the values of all iterations into the arrays, one of these arrays is inversed and Xored with the other array to produce new array that represent the chaotic sequence as shown in Fig.2

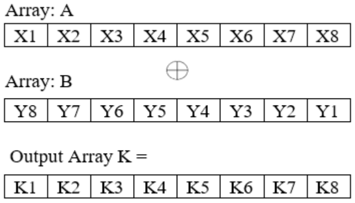


Figure 2: Chaotic sequence.

K is the key sequence that used for encryption process.

- ***Second approach*** In the second approach, we use logistic map in addition to cat map to produce key with larger key space. As in the above approach initial value of numbers between (0,1) are set for logistic and cat map, Lets x, y, z. Specific number of iterations are performed on all the three equations and produce the key with the same way as in first approach as shown in Fig.3 A, B, C are the iteration values of the arrays.

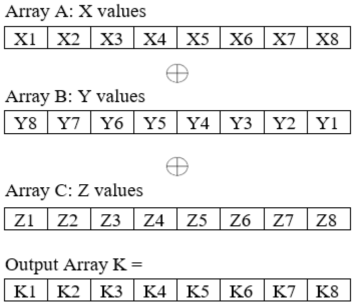


Figure 3: Chaotic sequence.

IV. Encryption Method

The whole process will be performed as the in following algorithm: Algorithm 1 video encryption with chaotic key generation and Fig.4 demonstrate the system steps

1) *The video data of the selected video for encryption is prepared for encryption.*
2) *Initial values of the key generator are randomly selected and set to all the equations of key generator.*
3) *Key generator will generate key sequence as long as the video data.*
4) *One-time pad stream cipher is performed on the data to be encrypted by xoring key sequence with the video data.*

5) *Encrypted video is constructed.* To obtain the decrypted video Xor operation is performed.And to use the method over networks initial values first securely distributed over the network by using public key encryption technique.

To obtain the decrypted video Xor operation is performed. And to use the method over networks initial values first securely distributed over the network by using public key encryption technique.

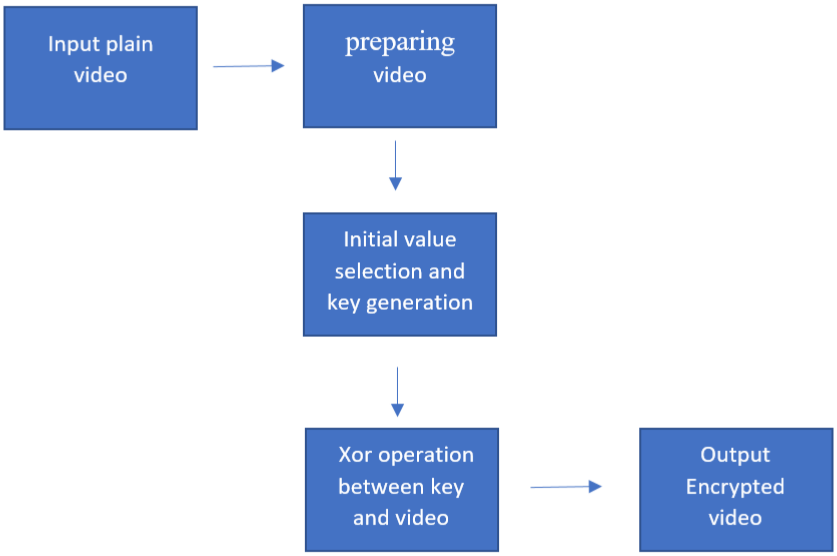

Input plain video
preparing video
Initial value selection and key generation
Xor operation between key and video
Output Encrypted video

Figure 4: Encryption process steps.

V. Analysis and Results

In this section result of some test and analysis of the encryption method will be discussed.

A. Key space

It is the number of possible keys that the key generator will produce, larger key space means more immune method especially against brute force attack. Since we use chaotic map in the proposed method, the initial value will play the role of key space each value will be digitally represented in sixty-four bits so the calculation of the key space for the two above approaches will be as the following: in the first approach Arnold cat map used alone and it needs two initial value, one for each equation, the number of possible keys will be $2^{64} \cdot 2^{64} = 2^{128}$ possible key.

In case of the second approach where combination of two chaotic maps, the possible keys will be increased because three initial value are used to form the key sequence, so the number of possible keys will be $2^{64} \cdot 2^{64} \cdot 2^{64} = 2^{192}$ possible key.

B. Visual appearance

Visual appearance of frame of video before and after the encryption.is shown in Fig.5 below.

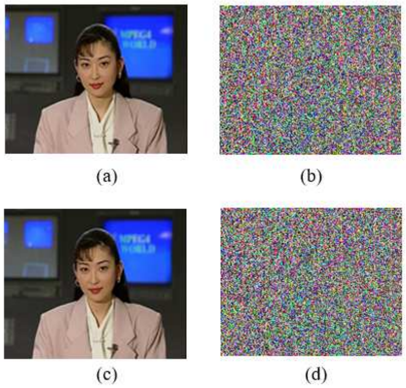


Figure 5: Visual appearance.(a), (c) represent the original frame before the encryption, (b) is the encrypted frame using cat map only while (d) is the encrypted frame using the hybrid of cat and logistic maps.

TABLE I
ENCRYPTION TIME

Sample Name	Size in byte	Cat map	Hybrid
Akiyo	3,802,258	0.311019	0.318570
Coastguard	4,182,478	0.345267	0.348602
Flower	4,752,808	0.396730	0.392885
Football	5,018,962	0.409540	0.406474
Average time	–	0.365639	0.366632

C. *Processing time*

Table I represents encryption time of video data for different sizes with cat map and hybrid algorithms.Table I also shows the encryption time for both approaches for different video samples,Table II shows the decryption time. It is noticed that both approaches have almost the same encryption and decryption time and that because in both approaches xor operation is performed to obtain encryption and decryption videos, Table III showing the time needed for generating sequence of key we notice that each approach has different key generation time due to the number of chaotic equations that used. In all three table the time calculated in seconds.

TABLE II
DECRYPTION TIME

Sample Name	Size in byte	Cat map	Hybrid
Akiyo	3,802,258	0.307106	0.307640
Coastguard	4,182,478	0.336871	0.339908
Flower	4,752,808	0.398499	0.395851
Football	5,018,962	0.408903	0.406416
Average time	–	0.362844	0.352453

TABLE III
KEY GENERATION TIME

Size in byte	Cat map	Hybrid
2000,000	0.258268	0.34623

D. Histogram

Histogram of frame refers to the intensity of pixel in the frame represented by graph. In original frame the pixel intensity is different and for good encryption the distribution of intensity should be almost uniform [13].

E. Mean Square Error (MSE)

It is a measurement tool used to find the difference between the original data and encrypted, decrypted data. Mathematically calculated using the following equation [14]:

$$MSE = \frac{1}{N}\sum_{i=0}^{N}[x(i,j) - \bar{x}(i,j)]^2, \tag{4}$$

where N is the number of pixels in the frame $x(i,j)$ is the original frame, $\bar{x}(i,j)$ is the encrypted or decrypted frame. When MSE is used for measuring the difference between the original and the encrypted frames high value of MSE mean immune to attack, but in case of using for measuring the difference between the original and decrypted should be minimum number and be perfect reconstruction if its equal to zero.

TABLE IV
MSE BETWEEN ORIGINAL AND ENCRYPTED

Sample Name	MSE for encryption Cat map	MSE for encryption hybrid
Akiyo	42759658774547.6	42428922353122.7
Coastguard	27736385912375.3	27331899433279.2
Flower	39749235359690.8	40438496221182.4
Football	18266940484023.1	17848552358063.5

TABLE V
MSE BETWEEN ORIGINAL AND DECRYPTED

Sample Name	MSE for encryption Cat map	MSE for encryption hybrid
Akiyo	0	0
Coastguard	0	0
Flower	0	0
Football	0	0

F. Peak Signal to Noise Ratio (PSNR)

Peak signal to nose ratio used for measuring the quality of the video been encrypted in case of measuring for encryption. Small number means better encryption and in case of decryption high number means better decryption and become perfect reconstruction when the MSE equal to zero which result infinity value for PSNR. PSNR mathematically calculated as [15]:

$$PSNR = 10Log(\frac{max^2}{MSE}), \tag{5}$$

Where *max* is the max possible value for the pixel. Table VI shows PSNR of the encryption, Table VII shows PSNR of the decryption. Table VIII shows PSNR to our method and the method that used in [7].

As seen from Table VIII, the average PSNR results of the suggested method is smaller than that of the method in [7], which indicates that the good security characteristic of the proposed method.

TABLE VI
PSNR OF ENCRYPTION

Sample Name	PSNR for encryption Cat map	PSNR for encryption hybrid
Akiyo	8.1840	8.2177
Coastguard	10.0638	10.1276
Flower	8.5011	8.4264
Football	11.8777	11.9783

TABLE VII
PSNR OF DECRYPTION

Sample Name	PSNR for encryption Cat map	PSNR for encryption hybrid
Akiyo	max	max
Coastguard	max	max
Flower	max	max
Football	max	max

TABLE VIII
COMPARISON OF PSNR BETWEEN SUGGESTED METHOD AND METHOD OF [7]

Sample Name	PSNR for encryption Cat map	PSNR for encryption hybrid	Method in ref [7]
Coastguard	10.06	10.12	11.37
Foreman	8.15	8.13	7.95
Mobile	6.9	6.9	7.65
Average	8.37	8.38	8.99

VI. CONCLUSION

In this paper video encryption method is proposed based on stream cipher and chaotic system as a key generator of one-time pad key with two different key generation approaches. The experimental result demonstrates that the both proposed approaches are secure, and the reconstructed video is perfect with MSE equal to zero and maximum value for PSNR. The results of PSNR test also show that proposed method has smaller value than in the method of [7]. First approach is faster in key generation time due to only use cat map as key generation which is simple equations and require short execution time. The second approach present larger key space because of it uses of three initial values two for cat map equations and one for logistic map, this increase in the number of initial values and the number of equations lead to increase the key generation time. For future work this method can be applied over network to provide secure video exchange and can be attached with text-based chat application as feature for secure media exchange.

REFERENCES

[1] Babatunde .AN, Jimoh. RG, Abikoye. OC, "Survey of Video Encryption Algorithms", Covenant Journal of Informatics and Communication Technology, vol. 5, No.1 ,2017.

[2] au Deshmukh, Pooja Kolhe, Vaishali, "Modified AES based algorithm for MPEG video encryption", International Conference on Information Communication and Embedded Systems (ICICES), PP 1-5,2014.

[3] Yang, Shuguo Sun, Shenghe, "A video encryption method based on chaotic maps in DCT domain", Progress in natural science, vol. 18, No.10, 2008.

[4] Shang, Fang Sun, Kehui Cai, Yongqi, "An efficient MPEG video encryption scheme based on chaotic cipher", Congress on Image and Signal Processing, PP 12-16, 2008.

[5] Lei, BY Lo, KT Lei, Haiju, "A new H. 264 video encryption scheme based on chaotic cipher", International Conference on Communications, Circuits and Systems, PP 373_377, 2010.

[6] Liang, Yuan Guo, Ke Li, JianPing, "An improved video encryption method design", International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), PP 95_99, 2013.

[7] Fei Peng, Han-yun Li, Min Long, "An Effective Selective Encryption Scheme for HEVC based on Rossler Chaotic System", International Symposium on Nonlinear Theory and its Applications International Symposium on Nonlinear Theory and its Applications, 2015

[8] Ibrahem, Mahmood Khalel Kassim, Hussein Ali, "VoIP Speech Encryption System Using Stream Cipher with Chaotic Key Generator", Journal of Fundamental and Applied Sciences, vol.10, No 65, PP.204_210, 2018

[9] Makris, George Antoniou, Ioannis, "Cryptography with chaos", Proceedings of the 5th Chaotic Modeling and Simulation International Conference, PP 12-15, 2012.

[10] Zhang, Jian Zhu, Yinxia Zhu, Hongpeng Cheng, Jian, "Some improvements to logistic map for chaotic signal generator", International Conference on Computer and Communications (ICCC), PP 1090-1093 2017.

[11] Prusty, Agyan Kumar Pattanaik, Asutosh Mishra, Swastik, "An image encryption & decryption approach based on pixel shuffling using Arnold Cat Map & Henon Map", International Conference on Advanced Computing and Communication Systems (ICACCS), PP. 1_6, 2013.

[12] Kabi, Kunal Kumar Pradhan, Chittaranjan Saha, Bidyut Jyoti Bisoi, Ajay Kumar, "Comparative study of image encryption using 2D chaotic map" , International Conference on Information Systems and Computer Networks (ISCON), PP.105_108, 2014.

[13] Somaraj, Shrija Hussain, Mohammed Ali, "Performance and Security Analysis for image encryption using Key image", Indian Journal of Science and Technology, vol. 8 issue 25, 2015.

[14] Rohith, S Bhat, KN Hari Sharma, A Nandini, "Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register", International Conference on Advances in Electronics Computers and Communications (ICAECC), PP.1_6,2014.

[15] Abdulgader, Ali Jumari, Kasmiran Ismail, Mahamod Idbeaa, Tarik, "Video Encryption Based on Chaotic Systems in the Compression Domain", International Journal on Advanced Science, Engineering and Information Technology, vol. 2 issue.1,2012.