IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

Secure Video Exchange System Based on Stream Cipher and Lorenz System

Laith Abdulhussein Hamood[1], Mahmood K. Ibrahem[2]

Iraqi Commission for Computers and Informatics, Informatics Institute for Postgraduate Studies, Baghdad, Iraq[1]

College of Information Engineering, Al-Nahrain University, Baghdad, Iraq[2]

Abstract: The huge development in communication, multimedia and networks technologies lead to huge increase in using and transmitting of digital video, with that development the need for securing of these digital data is increased. Video encryption is vastly used to provide security for digital video. In this paper a system for secure video exchange is suggested, which consist of proposed video encryption method based on stream cipher and chaotic system as a key generator. Chaotic systems have been used successfully with cryptography. Chaotic system has characteristic make it suitable to be used in encryption such as pseudo-randomness, and sensitivity to initial conditions. Secure Video exchange system with proposed video encryption method have been successfully designed and implemented, the analysis results and tests on the system demonstrated that the encryption method has good results in term of speed and security.

Keyword: Video encryption, Chaotic system, Stream cipher, Lorenz system

1. INTRODUCTION

In the previous decades' multimedia, networks and communication technologies have rapidly developed. This progress has led to enormous growth in using and transmitting of digital video over networks these video may be commercial or personal video and may contain sensitive data that should not revealed to unauthorized users. Video encryption considered as very effective way to provide protection for digital video [1], where encryption refer to the method that transform the original data into unintelligible and noisy data that cannot be read or understood by unauthorized users in order to deliver guard to the data been encrypted [2]. There are several traditional effective encryption methods but most of them not appropriate to be used for video encryption directly. In this paper we presented a Secure video exchange system with effective video encryption algorithm in term of speed and security which is based on one-time-pad key stream cipher and chaotic system.

2. LITERATURE SURVEY

In the field of encryption many researchers devoted them researches for developing methods for video encryption, in order to find out active methods for video encryption.

Shuguo Yang and Shenghe Sun [3] suggested technique for video encryption built on using of logistic map as key generator, where two logistic map are used to generate chaotic sequence used for scrambling the DCT coefficients of the frame and use precise formulation to encrypt the scrambling frame. **Ali Abdulgader, Kasmiran Jumari, Mahamod Ismail, Tarik Idbeaa [4]** they proposed encryption method based on logistic map as a key generator, by using three separated logistic maps where their initial values are diverse. A sequence of pseudo random number is produced using the outputs for all the three logistic maps this sequence used as encryption key, whereas alternative key built on specific formulation is used for permutation. DC and AC coefficient are chosen for the encryption process, encryption process performed by Xoring the key with coefficient and permutation of DC coefficient. **Jyoti S. Bowade, Pawan khade, Dr. M. M. Raghuwansh [5]** they suggested encryption process, based on Arnold cat map and chebyshev map where they used as a chaotic system for key generation. Encryption process performed in two phases; first step is shuffling the frames by using 4D Arnold cat map and the second step is the encryption of the data using 3D Arnold cat map.**W. Hamidouche et al [6]** in their proposed method they 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. **S. kotel, F. sbiaa, M. zeghid, M. machhout, A. baganne, R. tourki [7]** they suggested mixture encryption method use modified AES encryption algorithm, they use AES in CTR mode where CTR mode is faster but over lower security. And to improve the CTR mode security they propose to use chaotic map in two parts; first part used to scramble the pixels, second part allocated to the AES Central module to process the encryption or decryption processes.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

3. CHAOTIC SYSTEM

3.1 Definition: Chaos system defined as a kind of complicated dynamic behaviors, it is produced from determined nonlinear discrete or continuous systems. Chaotic system has been established from several different research zones, such as mathematics, physics, which is nonlinear dynamic system that can be presented mathematically through precise formula called chaotic map or chaotic function. Chaotic maps divided into two types; continuous maps and discrete maps, an example of the discrete systems are Logistic map, and an example of continues system are the Lorenz system. Chaotic systems have sensitive reliant on initial conditions. If two initial points are started very near to each other, the space between their successive orbits under chaotic map departs exponentially [8][9].

3.2 Lorenz System: Lorenz system is a three-dimension chaotic map that first presented by Edward Lorenz as a simplified weather model. He presented that minor change in the starting points of climate model could produce huge difference in the resulting weather. That means any change even if very slight change in the starting condition lead to make change in output of the system, this called the sensitivity of the initial state [10]. Lorenz system has the characteristic of the chaotic system which mathematically represented in the three dimensional equations as the following [11]:

$$\frac{dx}{dt} = \sigma(y - x) \ldots\ldots\ldots\ldots\ldots\ldots$$

$$\frac{dy}{dt} = x(p - z) - y \ldots\ldots\ldots\ldots\ldots \quad (1)$$

$$\frac{dz}{dt} = xy - \beta z \ldots\ldots\ldots\ldots\ldots\ldots$$

Where (σ, p, β) are the parameters of Lorenz system and their values as the follow $(\sigma = 10, p = 28, \beta = 8/3)$. And (x, y, z) are the initial values, and all of the three value are between zero and one, where t is the time. Figure 1 show the Lorenz attractor.

Figure 1: The Lorenz Attractor

4. SECURE VIDEO EXCHANGE SYSTEM

The proposed system consists of three main stages (user authentication, chaotic initial value distribution, encryption/decryption stage). Figure 2 illustrate the system stages.

4.1 User Authentication Stage

The user of the system tries to communicate securely with server by using public key encryption in order to obtain secure key distribution. RSA algorithm is selected to provide secure distribution for the secret key. Successful login requires before using the system, user first create an account into the system by filling in some information and send it to the server. The server authenticates the user info and send its public key to the user. After receiving the public key, user generate his key pair and send his public key to the server to be used in key generation stage, the final step of this stage is to update online user list.

4.2 Initial Value Distribution

Initial value is the seed that used in key generation process, in the suggested system the initial value playing the role of secret key, the proposed system used symmetric encryption technique, in this stage public key encryption is used to distribute the secret key as in the following scenario: user A ask for private communication with user B, where user A select the user who want to communicate with from its online list, message contain sender and receiver id info

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

encrypted using server public key and send to the server as request message, server receive decrypt the message and send the request to the appropriate user. If the second user accept the request the server will generate random initial values, and generate two messages contain generated initial values each message is encrypted with intended user public key. User receive the message and decrypt it with its private key.

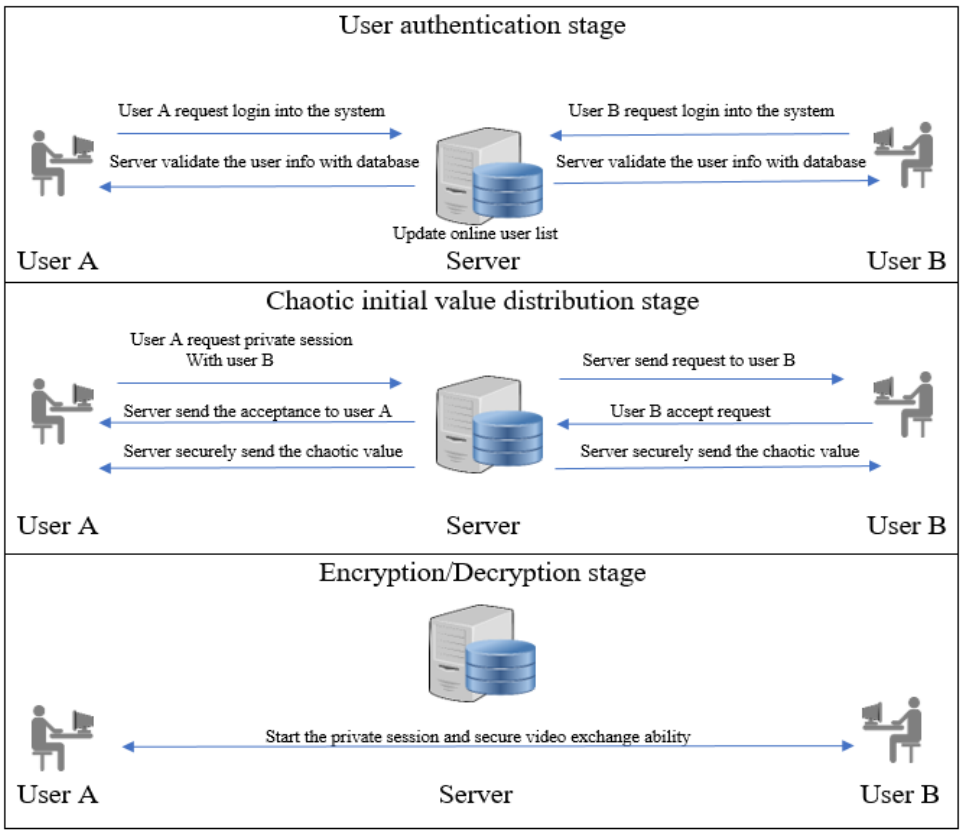


Figure 2: the proposed system stages

4.3 Encryption /Decryption Process

1.Encryption process

A. the user who want to send the video securely, select the video from his device, the system will prepare the video for encryption by extracting all the video data.

B. key is generated as follows:

Lorenz system is a differential equations system which containing of three dimensional equations and cannot straight get the values because it has differential and need to be solved by using Runge Kutta (RK4) method with 4th order. Runge Kutta (RK4) can be presented as [12]:

Let the differential equation of Lorenz system $\frac{dx}{dt}$ =(x,y,z) with initial values $\frac{dx}{dt}$ = x0 , $\frac{dy}{dt}$ = y0 , $\frac{dz}{dt}$ = z0 , then the approximate solution of $\frac{dx}{dt}$ using Runge Kutta is given by:

$$\mathbf{x_{n+1}} = \mathbf{x_n} + \frac{\mathbf{h}}{\mathbf{6}} * [\mathbf{k_1} + \mathbf{2k_2} + \mathbf{2k_3} + \mathbf{k_4}],\ \text{tn+1 =tn +h} \quad \ldots\ldots\ldots \quad \textbf{(2)}$$

Where xn+1 is the Runge Kutta approximation of $\frac{dx}{dt}$, h is the interval size ,t is the time, and

$$\mathbf{k_1} = \mathbf{f}(\mathbf{x_n}, \mathbf{y_n}, \mathbf{z_n}) \ldots\ldots\ldots\ldots \quad \textbf{(3)}$$

$$\mathbf{k_2} = \mathbf{f}(\mathbf{x_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_1}, \mathbf{y_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_1}, \mathbf{z_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_1}) \ldots\ldots\ldots\ldots \quad \textbf{(4)}$$

$$\mathbf{k_3} = \mathbf{f}(\mathbf{x_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_2}, \mathbf{y_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_2}, \mathbf{z_n} + \frac{\mathbf{h}}{\mathbf{2}}\ \mathbf{k_2}) \ldots\ldots\ldots\ldots \quad \textbf{(5)}$$

$$\mathbf{k_4} = \mathbf{f}(\mathbf{x_n} + \mathbf{hk_3}, \mathbf{y_n} + \mathbf{hk_3}, \mathbf{z_n} + \mathbf{hk_3}) \ldots\ldots\ldots\ldots \quad \textbf{(6)}$$

And calculating y_{n+1} and z_{n+1} by using the same equations of RK4 that used in calculating of x_{n+1} but replacing equation $\frac{dx}{dt}$ with $\frac{dy}{dt}$ or $\frac{dz}{dt}$. and the value of h is equal to (0.5). To obtain the key sequence in this method each iteration will produce three 64 bit values represented in double values, these double values will be an input to the next

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

iteration, and each value will be inserted into array, after the end of iteration one of the three arrays is reversed and Xored with other arrays producing the key sequence. Figure 3 illustrate the key generation process by using Lorenz system.

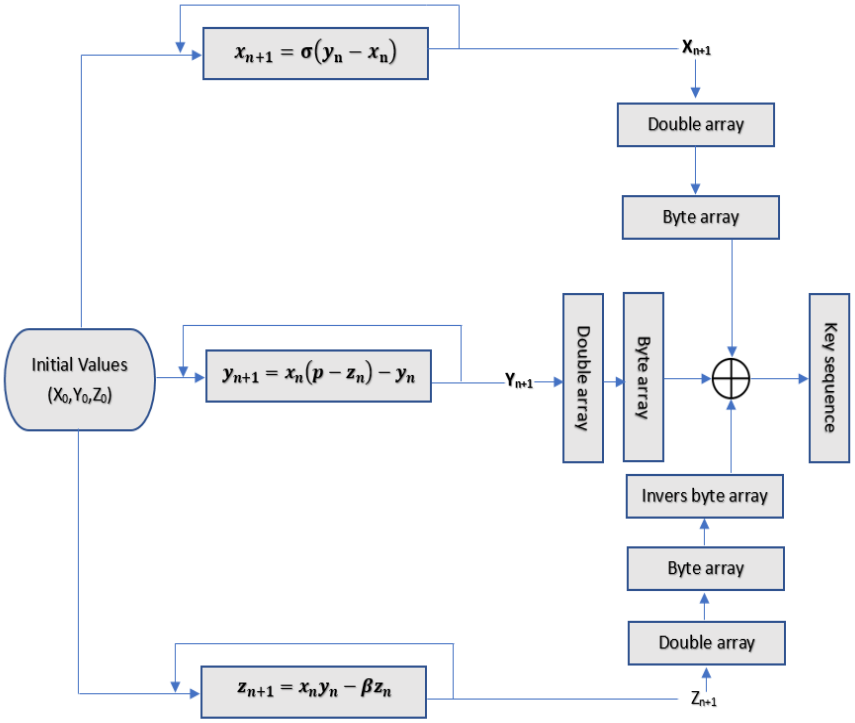


Figure 3: key Generation Process using Lorenz System

C. Xor operation is performed between the video data and the key sequence that generated in earlier step.
D. After encryption, encrypted video is sent to the Receiver. Figure 4 shows the encryption process.

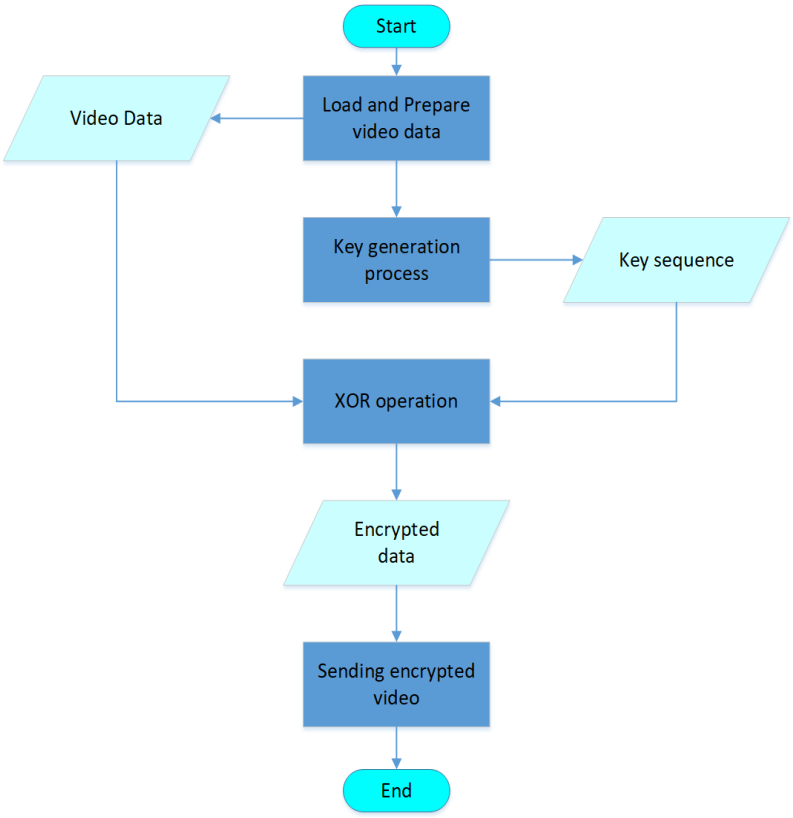


Figure 4: The Encryption Process.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

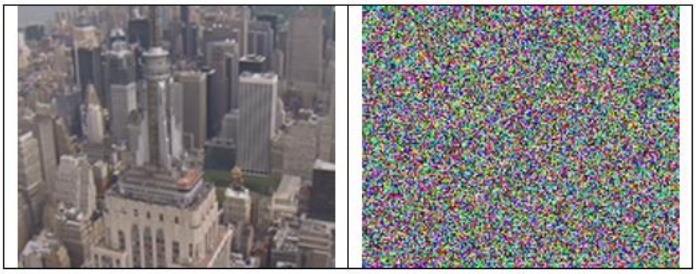
Vol. 5, Issue 9, September 2018

2. Decryption Process

A. The receiver receives the encrypted video, and hold it in one-dimension array for decryption.
B. User B has the same initial value as user A, so he generates the same key using the method of key generation mention in step B of encryption process.
C. Decryption process is the same as encryption process where decrypted video is XORed with key sequence to generate the decrypted video.
D. The final step is to store the video in User B device.

5. ANALYSIS AND RESULTS

5.1 Visual appearance: Visual appearance of frame of video before and after the encryption, is shown in Figure 5



a b

Figure 5: a Is the Original Frame, b Is the Encrypted Frame

5.2 Key Space: Key space refer to the number of keys that the key generator could produce, large key space is an indicator to more immune encryption method especially against brute force attack [12]. In the suggested system chaotic map is used as a key generator, the initial chaotic value will act as an encryption key, each value will be digitally represented in 64 bits, so the key space of the suggested encryption system equal to $2^{64}*2^{64}*2^{64}=2^{192}$ possible keys.

5.3 Processing Time: It is the needed time for encryption and decryption processes. Processing time is important as an indicator for the speed of the encryption method, where shorter time is referring to faster method Table 1 shows encryption for the proposed encryption method, Table 2 shows the decryption time, Table 3 is encryption time comparison between the proposed method and AES 256 and AES 128, table 4 is the decryption time comparison between the proposed method and AES 256 and AES 128.

Table 1 shows encryption time for the proposed encryption method

Num	Video name	Size in bytes	Encryption time	Key generation time	Total encryption time
1	Akiyo	3,802,258	0.3073681	0.7961095	1.1034776
2	Coastguard	4,182,478	0.3548285	0.8544178	1.2092463
3	City	4,752,808	0.3969622	0.9954591	1.3924213
4	Football	5,018,962	0.4121108	1.198968	1.6110788
ave		4,439,127	0.3678174	0.9612386	1.329056

Table 2 shows decryption time for the proposed encryption method

Num	Video name	Size in bytes	Decryption time	Key generation time	Total decryption time
1	Akiyo	3,802,258	0.3020554	0.7891097	1.0911651
2	Coastguard	4,182,478	0.3729606	0.861126	1.2340866
3	City	4,752,808	0.3729606	0.9965173	1.3694779
4	Football	5,018,962	0.4026468	1.203713	1.6063598
ave		4,439,127	0.36265585	0.9626165	1.3252723

Table 3 shows encryption time comparison between the proposed method and AES 256 and AES 128

Num	Video name	Size in bytes	Total encryption time	AES 256 encryption time	AES 128 encryption time
1	Akiyo	3,802,258	1.1034776	3.1246853	2.4265017
2	Coastguard	4,182,478	1.2092463	3.2936659	2.5335269
3	City	4,752,808	1.3924213	3.545526	2.797815
4	Football	5,018,962	1.6110788	3.8047467	3.0332898

DOI 10.17148/IARJSET.2018.595

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

ave		4,439,127	1.329056	3.442155975	2.6977833

Table 4 shows decryption time comparison between the proposed method and AES 256 and AES 128

Num	Video name	Size in bytes	Total decryption time	AES 256 decryption time	AES 128 decryption time
1	Akiyo	3,802,258	1.0911651	3.195041	2.4100754
2	Coastguard	4,182,478	1.2340866	3.285127	3.5123642
3	City	4,752,808	1.3694779	3.576354	2.782761
4	Football	5,018,962	1.6063598	3.788769	3.0027198
ave		4,439,127	1.3252723	3.46132275	2.9269801

The performance of an encryption algorithm can be determined by calculating Encryption Throughput (ET) which can be define as following

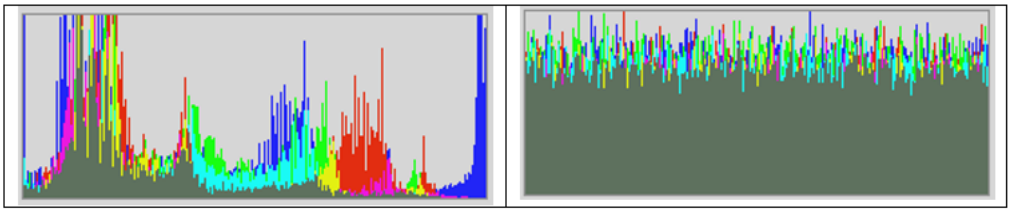
ET=Data size(Byte)/ Encryption time(millisecond) ……. (7)

Table 5 shows encryption throughput comparison between proposed method and AES 256 and AES 128.

Table 5 encryption throughput

	Proposed method	AES 256	AES 128
Encryption	3340.2	1289.7	1645.9
Decryption	3350.2	1282.6	1517.1

5.4 histogram: Histogram of frame refers to the intensity of pixel in the frame represented by graph. Histogram of good encryption algorithm should be different from the original and give no clue to statistically attack the encrypted frame [13]. Figure 6 Show the histogram of original and encrypted frames. The results of the histogram show that the encrypted frame histogram is different from the original and show, no relation which mean that it is immune against statistical attack.



a b

Figure 6: The Histogram of Original and Encrypted Frames.

5.5 Mean Square Error (MSE): this tool is used to determine the difference between the original data and encrypted, decrypted data. Mean Square Error Mathematically represented as in the following equation [14]:

$$\mathbf{MSE} = \frac{1}{N}\sum_{i-0}^{n-1}[x(i,j) - \bar{x}(i,j)]^2 \text{.....(8)}$$

where N is the number of pixels in the measured frame, x(i; j) is the original frame, $\bar{x}$(i; j) is the encrypted or decrypted frame.

The value of the MSE depend on how to us this tool, in case it used to find the difference between the original and encrypted frame, high value is better and refer to large difference, but when it used between the original and decrypted, smaller number is better and refer to the closest between the original frame and decrypted frame and in case of perfect reconstruction the MSE equal to zero. table 6 shows the MSE between the original and the encrypted data, table 7 shows the MSE between the original and the decrypted data.

Table 6: The MSE between the original and the encrypted data

Num	Test Samples	Proposed method
1	Akiyo	38335850255649.4
2	Coastguard	26223867457219.4
3	City	18556042021656.7
4	Football	17337230452561.3

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 9, September 2018

Table 7: The MSE between the original and the decrypted data

Num	Test Samples	Proposed method
1	Akiyo	zero
2	Coastguard	zero
3	City	zero
4	Football	zero

5.6 Peak Signal to Noise Ratio (PSNR): Peak signal to noise ratio used for measuring the quality of the video been encrypted when it used for encryption, small number means better encryption quality. PSNR can mathematically calculated as in the following equation [4]:

$$\mathbf{PSNR} = \mathbf{10log_{10}}\left(\frac{\mathbf{MAX^2}}{\mathbf{MSE}}\right)\ldots\ldots\ldots\ldots\ldots\ldots \quad \mathbf{(9)}$$

Where max is the max possible value for the pixel, MSE is mean square error. table 8 is the PSNR for proposed method.

Num	Test Samples	Proposed method
1	Akiyo	8.6583
2	Coastguard	10.3074
3	City	11.8095
4	Football	12.1046

CONCLUSION

In this paper secure video exchange system is proposed, with suggested encryption algorithm based on chaotic function as key generator of onetime pad key and stream cipher. The experimental result shows that the proposed encryption approaches is secure with high value for MSE and low value for PSNR for encrypted video, and has perfect reconstruction with MSE equal to zero due to lossless encryption based on bitwise XOR encryption. The proposed encryption method has fast encryption time and its faster than AES 256 and AES 128 in addition, the encryption method has large key space equal to 2^{192} which make it resistant to brute force attacks.For future work can use another chaotic map and study the impact on the encryption quality and the time, and study the ability of use the approach for real time video application.

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]. 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.
[5]. Jyoti S. Bowade, Pawan khade,M. M. Raghuwansh, "Technique of Video encryption/scrambling using chaotic functions and analysis", Journal of Emerging Technologies and Innovative Research (JETIR),Vol.2,Iss.6.2015.
[6]. W. Hamidouche, M. Farajallah, M. Raulet, O. D´eforges and S. El Assad," SELECTIVE VIDEO ENCRYPTION USING CHAOTIC SYSTEM IN THE SHVC EXTENSION", international conference acoustics, speech and signal processing (ICASSP), Pp. 1762-1766, 2015.
[7]. S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganna, R.Tourki," Efficient Hybrid Encryption System Based on Block Cipher and Chaos Generator" International Conference on Computer and Information Technology (CIT), Pp. 375-382, 2016.
[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]. Shujun Li, Xuan Zheng, Xuanqin Mou, Yuanlong Cai, "Chaotic Encryption Scheme for Real-Time Digital Video", Real-Time Imaging VI, Pp. 149-161, 2002.
[10]. Manel Dridi, Belgacem Bouallegue, Mohamed Ali, Abdellatif Mtibaa," An enhancement crypto-compression scheme for image Based on chaotic system", International Journal of Applied Engineering Research,Vol.11, Iss.7, Pp.4718-4725, 2016.
[11]. A.V. Prabu, S. Srinivasarao, Tholada Apparao, M. Jaganmohan, K. Babu Rao," Audio encryption in handsets", International Journal of Computer Applications, Vol.40, Iss.6, Pp. 40-45, 2012.
[12]. Fadhil S. Hasan," Speech Encryption using Fixed Point Chaos based Stream Cipher (FPC-SC)", Eng. &Tech. Journal, Vol.34, No.11,2016.
[13]. Shrija Somaraj, Mohammed Ali Hussain, "Performance and Security Analysis for Image Encryption using Key Image" , Indian Journal of Science and Technology, Vol 8,2015.
[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.