International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-4 Issue-13 December-2013

An Optimized Multikeying Chaotic Encryption for Real Time Applications

R. Tamijetchelvy[1], P. Sankaranarayanan[2]

Abstract

In recent years, the availability of wireless technologies has become prominent solution for next generation wireless networks (NGWN). Hence the demand for secure communication is an important research issue. Cryptography is recognized as the best method of data protection against active and passive attacks. Therefore a novel chaotic cryptographic scheme is proposed for real time communication. Chaos signals are random behaviour, continuous and sensitive dependence on initial conditions. However, it has been shown that most of these chaotic methods have a low level of security because of single keying concept. In this paper an optimized fast encryption scheme based on chaotic signal with multi key is justified for video frame. Simulation results show that the proposed chaotic encryption scheme outperforms the existing scheme in terms of considerable reduction in encryption and decryption time. The security of the proposed scheme is also analysed by various cryptanalysis attacks.

Keywords

Chaos, Multi-key, Diffusion, Confusion, Cryptanalysis, Iterations.

1. Introduction

Owing to ubiquity of different wireless technologies, user satisfaction is greatly affected by the factor such as security, mobility, quality of service, continuous connection anywhere, anytime and any service has become crucial factor nowadays. Hence, the future generation wireless networks aims to satisfy the user needs. With the development of heterogeneous and homogeneous network environment, Internet and multimedia technology including video, audio, image, and other application information has been transmitted over the untrusted wireless channel.

Perunthalaivar Kamarajar, Inst. of Engg. & Tech, India.
P. Sankaranarayanan, Bharathiyar College of Engg. & Tech, India.

The information passed through this medium are protected and should not give an opportunity for the attacker or illegal user to trace the sensitive information. Thus the network security of communication becomes more and more crucial factor. 3G cellular networks include controllability, reliability, credibility, confidentiality, integrity, and availability as well as being supervisory. For image, there are two most important secure methods. First method is the information hiding which includes watermarking, steganography etc. The second method is encryption technique which includes symmetric and asymmetric cryptography. For military applications high sensitive data are transmitted over wireless medium. Image encryption and video encryption has become an important research area for information and network security. Enhanced two channel optical chaotic communication [1] using isochronous synchronization with twin semiconductor lasers. Moreover, this idea can be extended to any communication systems using complex chaotic signals. Numerically demonstrated high speed [2] fiber optic transmission using four chaotic semiconductor laser and the properties of bandwidth enhancement, bit-error rate of the recovered message is evaluated for different fiber lengths.[3] Proposed an idea for improving the compression performance of an existing chaos-based joint compression and encryption scheme where the expansion of the cipher text is avoided, the better compression performance and execution efficiency is comparable. However, in Chaos concept, determinism is one of the basic principles and it is the belief that every action that happens as the result of preceding actions. Because of this deterministic nature, people can adopt chaos theory to illustrate the phenomenon of events happening in this world. A novel image scanning and transmission system [4] is proved to be efficient, where the traditional raster scan is replaced with chaotic scan. The encryption and spread spectrum capabilities are well suited for compressed sensing applications where the chaotic counter addressing the sensor array, based on a cellular automaton exhibits a pseudo-random chaotic behaviour and binary synchronization property. Later a new image encryption algorithm by combining the cat map and the standard mapping of conservative chaotic systems is proposed in [5]. Two parameters

are used to realize the scrambling encryption for images. This idea overcomes the periodicity of using cat mapping directly to encrypt the image. More ever [6] the 3D multi-chaotic map is presented to achieve higher security with random scan processing to increase the confusion process, the combinations of coupled map lattice model, tent map and logistic chaotic map are employed for high security diffusion process and also to improve the initial sensitivity. A new nonlinear chaotic algorithm (NCA) which uses power function [7] and tangent function for image encryption algorithm in a one-time-one password system. It is suitable for Internet image encryption and transmission applications and also supports wide range of applications. NCA proves to be efficient and shows the advantages of large key space and high-level security. The method can be used for encoding binary images using one-dimensional chaotic maps with the possibility of using [8] several keys such as the initial state, the external parameters and the number of iterations for different degrees of chaos corresponds to different values of positive Lyapunov exponent.

New chaos based secure communication system, information is carried across an AWGN channel has a pair of synchronized chaotic circuits. The security of the system is increased by XOR operation between the digital signal and the chaotic signal. Therefore XOR operation masks the information of both the signal efficiently [9]. The effect of this encryption scheme leads to cheaper and provides effectively for ensuring security and privacy in commercial electronics products.[10] Proposed a class of Feistel structure block encryption ciphers based on chaos using two chaotic maps namely exponential and logistic map. S-boxes are created by using chaotic maps and turns out very simple discretization procedure to generate secure S-boxes, than in the case of randomly constructed S-boxes which are unlikely to be secure. A system oriented analysis of chaos communication systems consist of lasers to all optical feedback is presented in [11]. Two codification methods are efficiently analysed they are external baseband and subcarrier modulation. The robustness of each codification method are subject to two cryptanalysis attack, filtering of the directly detected signal and the usage of an arbitrary receiver to synchronize and extract the message which is numerically evaluated through error counting progress. An attempt was made to include certain compression potential in the Baptista-type cipher by adaptively construct the lookup table according to the chance of happening of the plaintext symbols. The Cipher text is no longer than the plaintext, but the compression ratio still has a distance from the source entropy technique. This is because the chaotic search path frequently [12] domain on the partitions corresponding to irrelevant source symbols, the number of iterations is larger than necessary, and the compression ratio is not close to the source entropy. In recent years, there is a demand for increasing a complex trend of designing ciphers based on chaos is the important area in wireless domain. Because chaotic signals are highly sensitive to the initial condition and the system parameters. These properties are desirable in cryptography [13]. The knowledge on chaos signal and nonlinear dynamics can be applied in the field of network security. A chaos-based cipher considered by Baptista search the plaintext in the lookup table using a key dependent chaotic route and treats the number of iterations on the chaotic map as the cipher text.

The rest of this paper is organized as follows. Section II provides the overview of chaotic systems and explains why chaotic encryption is essential components of multimedia applications. Section III describes the proposed encryption algorithm architecture for both the encryption and decryption mechanism. Section IV demonstrates the simulation results and discussions of chaotic encryption with multi key technique. Section V analyses the various security attacks of the proposed system and finally section VI conclude the results of the proposed work and scope for future research.

2. Chaotic Maps – An Overview

Recent cryptographic techniques are mainly based on number theoretical and algebraically concepts. Chaos is another paradigm, which proves promising area nowadays. Chaos is a different field of nonlinear dynamics and has been widely analysed in recent years. The main key idea for applying chaotic algorithms to data, image, video or audio encryption is because of thefour following intrinsic characteristics of chaotic algorithms: Highly complex and nonlinear behaviours [14], Sensitive dependence on initial conditions, Sensitive Dependence on System Parameters and Ergodicity property.

2.1 Lorenz System

The Lorenz system of ordinary differential equations having chaotic solutions for certain parameter values and initial conditions. Lorenz chaotic system have a

classical high dimensional chaotic state is indubitable. The number of sequence made on either side varies unpredictably from one to the next as in fig. 2. The sequence in each lobe has many of the characteristics of a random sequence. The encrypted result proves to be this system has three main attractive advantages. Primarily the structure of lorenz system is more complex than the low dimensional chaotic systems. Therefore it is very difficult to forecast the chaotic sequences that need to encrypt. Second, the real value sequences of three system parameter can be used singly. Finally, all the three initial conditions and three control parameters of this system can be made larger than the low-dimensional chaotic system.

$dx / dt = \sigma (y - x)$
$dy / dt = x (\rho - z) - y$
$dz / dt = = xy - \beta z$ (1)

Here x, y and z are the system state,t is time and σ, β, ρ are the system parameters. σ = 10; b = 8=3; r = 28 as in Lorenz's original work published in year 1963.Changing the parameters, exotic behaviours such as exotic limit cycles linked through each other of intermittent chaos system.

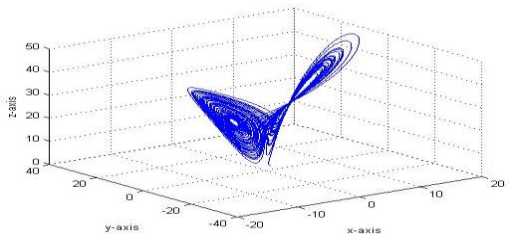

Figure 1: 3D View of Lorenz System

2.2 Rossler System

Proposed a series of prototype systems of ordinary differential equations in three dimensional and also in four dimensional systems for hyper chaos that is positive Lyapunov exponent.

$dx / dt = -y - z$
$dy / dt = x + ay$
$dz / dt = = bx - cz + xz$ (2)

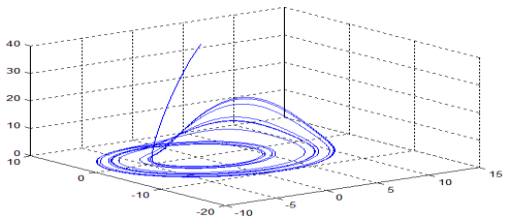

Figure 2: Phase of Rossler System

x, y, z are the three variables that change in the continuous time t and a, b, c are three parameters. This system is minimum for continuous chaos for at least three main reasons they are its phase space has the minimal dimension three [15], its nonlinearity is minimal because there is a single quadratic term as in fig. 2, and it generates a chaotic attractor with a single lobe, in contrast to the Lorenz attractor which has two lobes. The homoclinic system contains periodic and non-periodic orbits belonging to multiple horseshoes in terms of symbolic dynamics.

2.3 Chen System

In 1999, Chen found another classical chaotic attractor in a simple three-dimensional autonomous system Chen's system does not belong to this generalized Lorenz system family [16].

$dx / dt = a(y - x)$
$dy / dt = (c - a)x - xz + cy$
$dz / dt = xy - bz$ (3)

Where chaotic parameters a = 35, b = 3, c = 28.The strength of cryptography lies in choosing the keys which are secret parameters and necessary, used in encryption process. It should not be possible to guess the key by an intruder in the wireless medium. Since chaotic systems are very sensitive to initial conditions and system parameters, for a given set of parameters in chaotic regime, two close initial conditions lead the system into divergent trajectories as in fig.3.

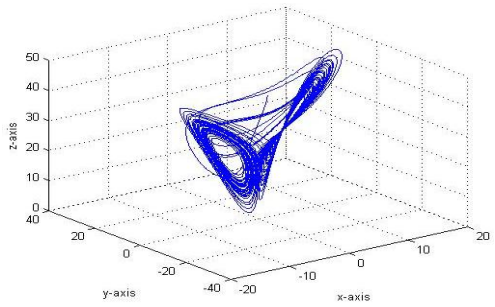

Figure 3: Chen System

2.4 Lu system

The hybrid synchronization behaviour in the Lu hyper chaotic system which drive system with the four state variables having identical equations. However, the initial condition on the drive system is different from that of the response system [17]. The two Lu systems are described by the following equations

$dx / dt = a(y - x) + yz$
$dy / dt = - xz + cy$
$dz / dt = xy - bz$ (4)

where x, y, z are the state variables and a, b, c are the real constants. When a = 36, b = 3, c = 20.

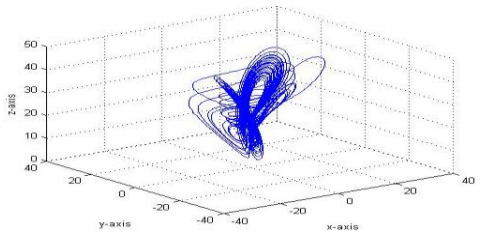

Figure 4: Phase of Lu System

The hybrid synchronization behaviour in hyper chaotic Lu system using a nonlinear active control method which is simple, efficient and easy to implement in practical applications as in fig. 4.

2.5 Henon System

The Hénonchaotic map is a discrete time dynamical system that exhibit chaotic behavior. The map is a simplified model of the Poincaré section of the Lorenz model. The initial point of the plane will either approach a set of points called Hénon strange attractor, or diverge to infinity.

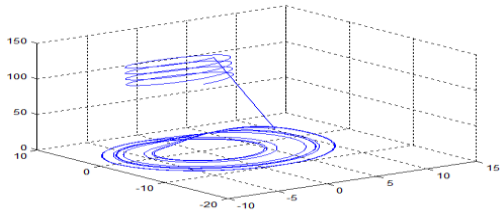

Figure 5: Henon Chaotic Map

$$dx / dt = a - (y2 - bz)$$
$$dy / dt = x$$
$$dz / dt = y \quad (5)$$

The map depends on two important parameters a and b, the value for the Hénon chaotic map have values of a = 1.4 and b = 0.3. For the classical values the Hénon map is chaotic as in fig.5.

3. Proposed Multi-key Chaotic Encryption

The proposed idea provides an optimized and efficient encryption and decryption process. The architecture of many chaotic based image encryption schemes have been proposed for single key and multi key techniques which mainly consistt of confusion (permutation) stage and diffusion stage.More ever, the confusion process is obtained by permutation as the only stage, while the diffusion process is merely found in the pixel value diffusion stage. However in most of the encryption schemes, the required numbers of confusion and diffusion iterations are unnecessarily larger to achieve a high level of security.Therefore the efficiency of the encryption process is thus downgraded.

3.1 Encryption and Decryption Process for Multi key Chaotic system

The encryption process of a colour video image in the proposed multi key chaotic algorithm is depicted in fig 6.Two different external keys of 16-byte (128 bits) are chosen for initial key processing for both confusion and diffusion process. These keys are processed independently to select one of the chaotic systems(Lorenz, Henon, Rosseler, chen or Lu).The original colour video is taken and split up into frames. The frames comprise of still image and the video frames contain identical pixel value with the neighbour pixels. Therefore it generally split up in to I frame, P frame and B frame such that the encryption redundancy is removed. The colour image frame is split up into RGB frame then each frame pixel position is confused by the generated chaotic sequence. The proposed work uses three chaotic systems Lorentz, Chen and Lu in the direction X, Y and Z. The first chaotic sequence is Lorentz system equation and its control parameters is given below

$$dx / dt = \sigma (y - x)$$
$$dy / dt = x (\rho - z) - y$$
$$dz / dt = = xy - \beta z \quad (6)$$

where the initial conditions are x(1)=1.1840,y(1)=1.3627,z(1)=1.2519, σ = 10,β = 8=3, ρ = 28. The parameters and the initial conditions together form a very large key space and thereby enhancing the security of the encryption process as shown in fig.6. The second chaotic sequence is Chen system and its control parameters are x (1) = 1, y (1) = 1, z(1) = 40, a = 35, b = 3, c = 28 for system equation given in (7).

$$dx / dt = a(y - x)$$
$$dy / dt = (c - a)x - xz + cy$$
$$dz / dt = xy - bz \quad (7)$$

Since the same parameters are used for both encryption and decryption process since the chaos scheme is symmetric. The confused pixel value is the diffused by another chaotic sequence with different key to make the encrypted image more complex.

dx / dt = a(y - x) + yz
dy / dt = - xz + cy
dz / dt = xy – bz (8)
where x (1)=1.1, y(1)=1.1, z(1)=40, a = 36, b = 3, c = 20. These three chaotic sequences are used to confuse the pixel position with the help of 128 bit key.

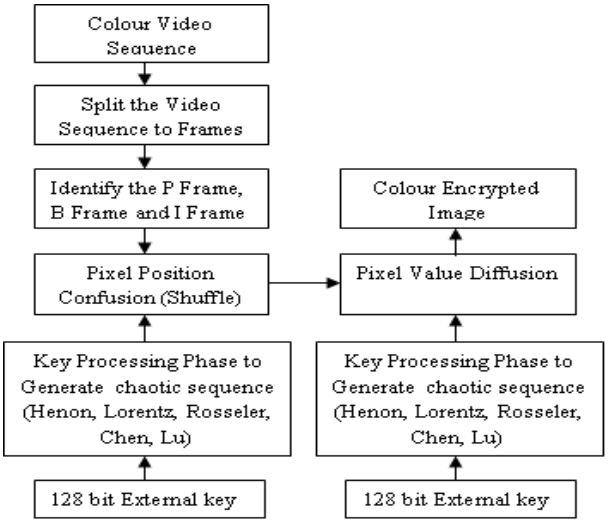

Figure 6: Encryption Process

The decryption process is the reverse process of encryption. The encrypted image is first diffused with the generated chaotic sequence which is then employed to confusion to get the original decrypted video file as in fig. 7.

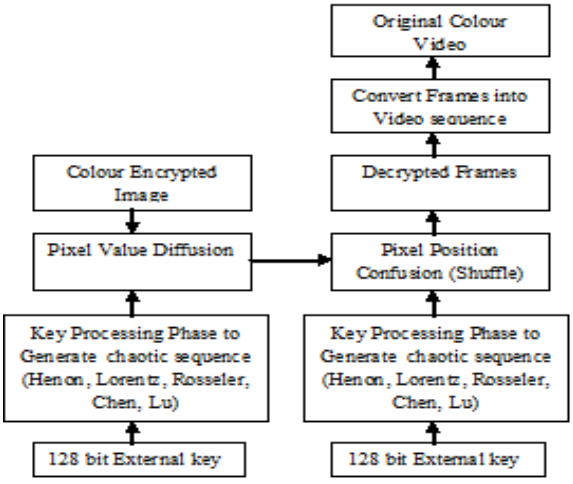

Figure 7: Decryption Process

3.2 Pre-treatment Process

An ideal chaotic sequence should have the following properties average value is equal to zero, auto correlation as a delta function and mutual correlation equal to zero. Therefore whole pre-treatment process should be carried out and is given by the following equation (9).

$$x_k(i) = 10^n x_k(i) - \text{round}(10^n x_k(i)) \quad (9)$$

where x, y and z are real value chaotic sequence.

4. Simulation Results and Discussions

This section provides the experimental results and analysis to show how the performance of the proposed cryptosystem is improved using multi key. The proposed video encryption scheme uses Lorenz, Chen and Lu chaotic system for pixel position confusion and diffusion for generating multiple keys chaotically. The test video taken for encryption is the Mountain View colour image of size 256x256.As one of the frame image is shown in fig. 8. The colour image frame is split up into RGB frame and its corresponding RGB histogram analysis is depicted and illustrated in fig. 8.

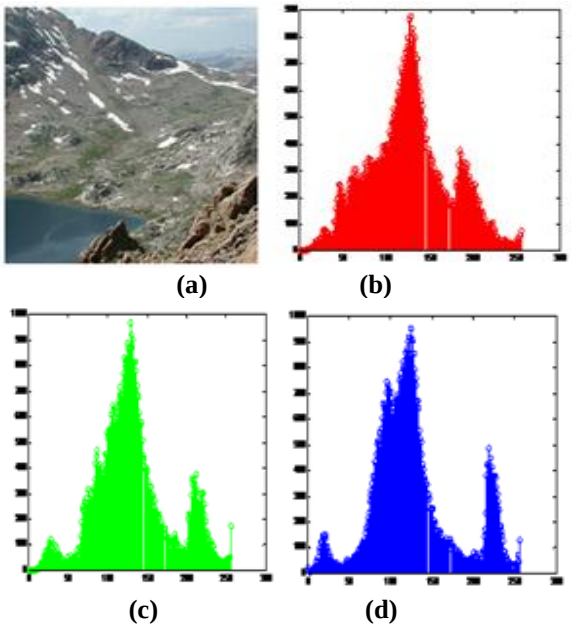

Figure 8: (a) Original Image Frame (b) Red Frame Histogram (c) Green Frame Histogram (d) Blue Frame Histogram

The first phase of encryption process is the confusion and it is done by Lorenz, Lu and Chen chaotic system

as mentioned in equation (1), (3) and (4) and mentioned chaotic sequence for Lorenz, chen and lu is demonstrated in fig. 11, fig. 12 and fig. 13. The input to chaotic sequence generator is the 128 bit key stream.

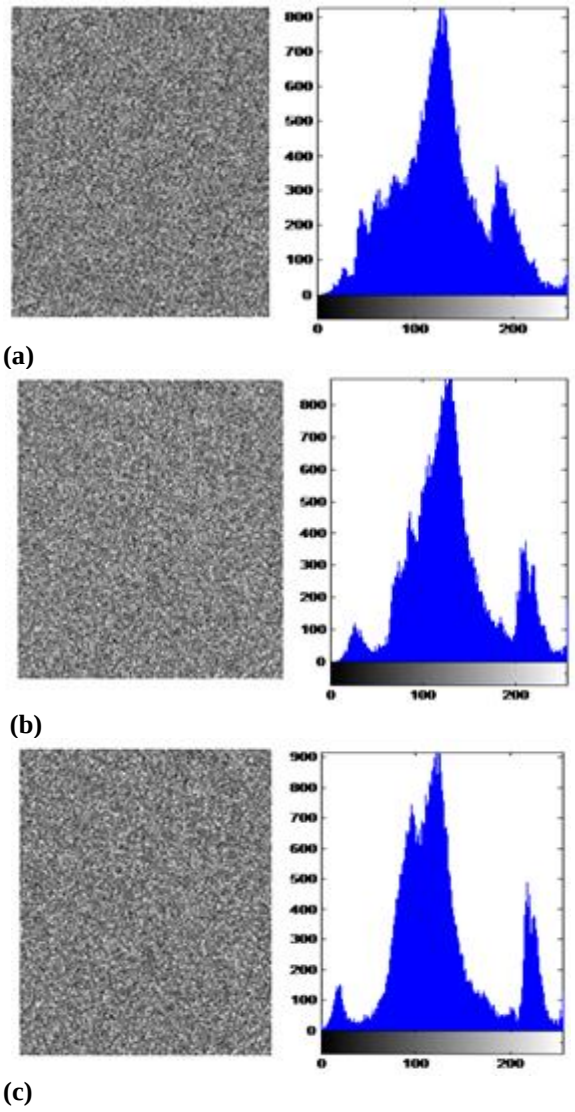

Figure 9: (a) Confused Red Frame (b) Confused Green Frame (c) Confused Blue Frame

Based on the generated chaotic sequence, the image pixel position are confused. The confused image frames and its corresponding histogram are illustrated in fig. 9.

key1=mod((key(1)+key(2)+key(3)+key(4)+key(5)+ key(6)+key(7)+key(8)+key(9)+key(10)+key(11)+key (12)+key(13)+key(14)+key(15)+key(16)),10)

key2=mod(bitxor(key(1),key(2)),10)

key3=mod((key(4)*key(8)+key(10)),10) (7)

The nature of the image is uncorrelated with the original one but the histogram analysis is correlated with the original image. Therefore confusion process only changes the external outlook of the image not the real. The whole pre-treatment process should be carried out in order to make uncorrelated with the one

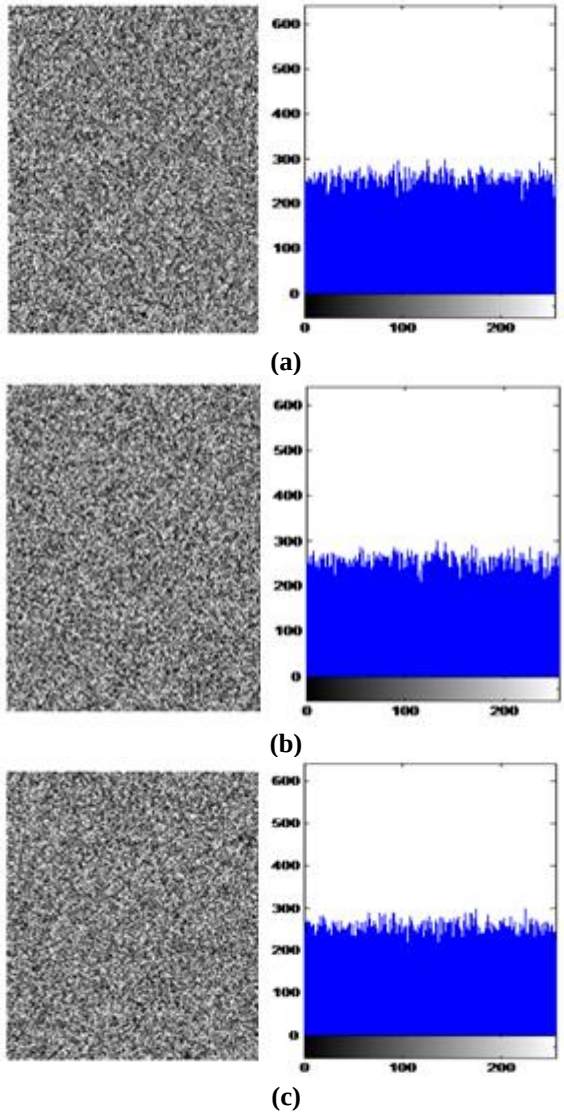

Figure 10: (a) Diffused Red Frame (b) Diffused Green Frame (c) Diffused d Blue Frame

original image.The second phase of encryption process is the diffusion process. The resultant is the

encrypted cipher image which is highly complex and unbreakable as shown in fig. 10. The finally concatenated Red, Green and Blue frames are shon in fig. 14.

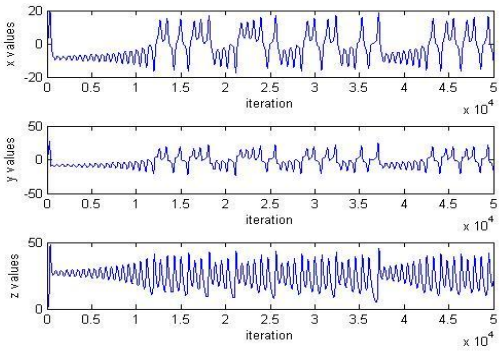

Figure 11: Real value Chaos sequences of Lorenz system

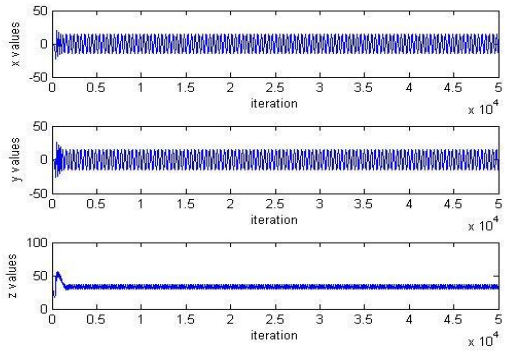

Figure 12: Real value Chaos sequences of Chen system

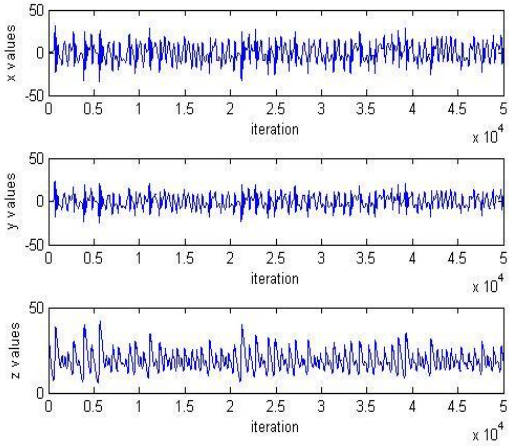

Figure 13: Real value Chaos sequences of Lu system

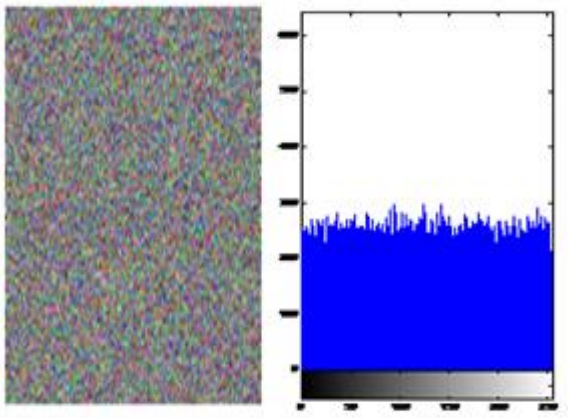

Figure 14: Encrypted Image and its Histogram

Decryption process is the reverse of Encryption phase. First the encrypted cipher image is diffused using the chaotic sequence generated with external 128 bit key. The resultant image obtained, whose pixel value is shuffled. Therefore reverse confusion process is carried out with the help of another generated chaotic sequence with external key.

(a) **(b)**

(c)

Figure 15: (a) Decrypted Red frame (b) Decrypted Green frame (c) Decrypted Blue frame

The final output is the original decrypted image which is then converted to video file. The corresponding decrypted frames are shown in fig. 15.

(a) **(b)**

Figure 16: (a) Original Image (b) Retrieved Original image

The finally decrypted image is as same as the original image. Hence the proposed system proves to be more efficient and secure for both real time and non-real applications.

5. Security Analysis

The robustness of the proposed multi key chaotic scheme is analyzed with various tests. Key space analysis and encryption time analysis were carried out to exhibit the reasonable security of the proposed scheme. For a high secure image encryption, the key stream should be large enough to make impossible for brute force attack. A 16 byte (128 bit) key is used to produce a long key stream with combined Chen, Lorentz and Lu methods for confusion and diffusion of image pixel. The long and different key distribution scheme proposes to encrypt video image with multi-keys, which increase the security level.

The encryption time of the video image should not be large enough for real time application processing. It has been stated that the encryption time is greatly affected by pixel by pixel approach and reduced for block-by-block approach. Greater the block size, will yield greater reduction in encryption time. But there is a trade-off between the block size and security. When the block size increases, the encryption time increases but the level of security is reduced. Therefore an optimal block size is preferred for image encryption.

6. Conclusion and Future Work

An efficient chaotic system based video image encryption schemes have been demonstrated. The proposed work is achieved by modifying and optimizing some existing chaotic cryptographic schemes with multi key concept. For a good and complex cipher principle, the combined confusion and diffusion schemes are employed in the proposed work. Experimental results prove that the presented work produces very complex cipher with more number of iterations and long key stream and robust against various attacks. It is concluded that the proposed cryptosystem is very much suitable for real-time transmission.

The future work aims towards image storage capacity or transmission lossless or lossy compression is usually employed so as to reduce the information storage which is transmitted. Since video files have more number of image frames hence compression is necessary for such applications. More ever image compression techniques such as Discrete Cosine Transform, Discrete Wavelet Transform etc. can be integrated with the proposed scheme to have acceptable encrypted cipher image. A few points with recommended, usually a large number of iterations rounds guarantee to achieve sufficient security and thus result in disappointing encryption speed.

References

[1] Nianqiang Li, Wei Pan, Lianshan Yan, Bin Luo, XihuaZou, Shuiying Xiang , "Enhanced Two-Channel Optical Chaotic Communication Using Isochronous Synchronization", Selected Topics in Quantum Electronics, IEEE Journal Vol:19 , Issue: 4 , 2013.

[2] Nianqiang Li, Wei Pan, Bin Luo , Lianshan Yan , XihuaZou, Ning Jiang, Shuiying Xiang ," High Bit Rate Fiber-Optic Transmission Using a Four-Chaotic-Semiconductor-Laser Scheme", Photonics Technology Letters, IEEE, 2012.

[3] Jianyong Chen, Junwei Zhou, and Kwok-Wo Wong," A Modified Chaos-Based Joint Compression and Encryption Scheme", IEEE Transactions on Circuits and Systems—II: Express Briefs, Vol. 58, No. 2, February 2011.

[4] RaduDogaru, IoanaDogaru, and Hyongsuk Kim," Chaotic Scan: A Low Complexity Video Transmission System for Efficiently Sending Relevant Image Features", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 20, No. 2, February 2010.

[5] Wang Tao,ZhangHan,LiZhaohui,Zhang Qing-hua," The Images Encryption Algorithm Based on the Multi-Chaotic Systems", International

Conference on Multimedia Information Networking and Security, 2009.
[6] YikuiZhai, Shuyong Lin, Qiong Zhang, " Improving Image Encryption Using Multi-chaotic Map", Workshop on Power Electronics and Intelligent Transportation System, 2008.
[7] HaojiangGao, Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption", Chaos, Solitons and Fractals 29 (2006) 393–399, 2005 Published by Elsevier Ltd.
[8] FethiBelkhouche and UvaisQidwai,"Binary image encoding using 1D chaotic maps", IEEE Proceeding, April 2003.
[9] K. Murali, Haiyang Yu, VinayVaradan and Henry Leung," Secure Communication using a Chaos Based Signal Encryption Scheme", IEEE Transactions on Consumer Electronics, Vol. 47, No. 4, November 2001.
[10] GoceJakimoski and LjupcoKocarev," Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps", IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications, Vol. 48, No. 2, February 2001.
[11] Bogris, A., Argyris, A. , Syvridis, D. ," Encryption Efficiency Analysis of ChaoticCommunication Systems Based on Photonic Integrated Chaotic Circuits", Quantum Electronics, IEEE Journal Vol:46 , Issue: 10 , 2010.
[12] K. W. Wong and C. H. Yuen, "Embedding compression in chaos-based cryptography," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 55, no. 11, pp. 1193–1197, Nov. 2008.
[13] M. S. Baptista, "Cryptography with chaos," Phys. Lett. A, vol. 240, no. 1/2, pp. 50–54, Mar. 1998.
[14] Hephzibah Kezia, Gnanou Florence Sudha," Encryption of Digital Video Based on Lorenz", ADCOM, IEEE Conference, 2008.
[15] Pierre Gaspard," Rossler systems," Encyclopedia of Nonlinear Science, Alwyn Scott, Editor, (Routledge, New York, 2005) pp. 808-811.
[16] Jinhu Lu, Guanrong Chen," A New Chaotic Attractor Coined", International Journal of Bifurcation and Chaos, Vol. 12, No. 3 (2002) 659-661.
[17] K.SebastianSudheer, M Sabir," Hybrid synchronization of hyperchaotic Lu system", PRAMANA journal of physics, Indian Academy of Sciences Vol. 73, No. 4 October 2009,pp. 781-786.

R. Tamijetchelvy residing in Karaikal, Pondicherry. Received B.Tech Degree in Pondicherry Engineering College (2004) and obtained Master degree affiliated to Anna University (2007). Currently Part time Ph.D Research Scholar in Pondicherry Engineering College and also working as an Assistant Professor in PKIET, Karaikal. Research interest includes Image Processing, Mobility management in wireless networks and Cryptography.

P.Sankaranarayanan residing in Karaikal. Received B. Tech and MBA Degree in Pondicherry University, Master degree in PRIST University. Currently working as an Assistant Professor in Bharathiyar College of Engineering and Technology, Karaikal. Research interest includes Image Processing, Wireless networks and Cryptography.