www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11985-11989

An Optimized Image Encryption Technique for Multikey conservative chaotic system

[1]P.T.Bhuvana, [2]L.Thirumal,
[1]PG scholar VaruvanVadivelan Institute of Technology, Dharmapuri,
[2]Assistant Professor VaruvanVadivelan Institute of Technology Dharmapuri,
bhuvanaraj91@gmail.com thirumal09@gmail.com

Abstract— ***In recent years of wireless access communication, the internet and other computer communication technologies are radically changing the ways of communication and information exchanging source. However, along with speed, efficiency and cost-saving benefits of the digital revolution, there exists a new challenge for the security and privacy of communication of information. Hence cryptographic algorithms are efficient tool for encryption. In this paper a new color image encryption algorithm is proposed by combining Lorentz and Rossler attractor with multi-key concept for conservative chaotic system. Also, the pixel values of the plain image are modified randomly using confusion and diffusion process to strengthen the image security. The resultant encrypted image is compared with various results obtained using single and multi key algorithms. The proposed algorithms is also analyzed under different critical attacks and the results show that the proposed system has a better efficiency, image confidentiality, high encryption and decryption speed.***

Keywords— **Encryption, Lorentz, Rossler attractor, Multi-key, Confusion, Diffusion.**

I. INTRODUCTION

Today, the internet is a decentralized network of networks. Anyone can connect to the internet and can share any type of information in the form of data, image, videos, etc, even if it is potentially detrimental to the unsuspecting recipient. This places a large burden on each and every organization that has internet connectivity to be responsible to ensure security. Thus Cryptography is the strongest tool for implementing security services. Cryptography is also used in complicated protocols that help to achieve different security services, thus called as security protocols. Hence a cryptographically-based mechanism becomes the building blocks of computer security. One of the mechanisms is encryption technique. Many different encryption algorithms have been projected in recent years as possible solutions for the protection of digital images. But some of these methods became week against certain type of attacks and criteria. At hand, there are many image encryption techniques such as Tangram algorithm [1], Arnold map [2], Baker’s transformation [3], affine transformation [4]. In some of this technique, the secret key and the algorithm cannot be efficiently separated. Hence, this does not satisfy the necessity of modern cryptographic mechanism and prone to various attacks. In present years, the image encryption based on the chaotic dynamics system has been proliferated to overcome above disadvantages. Zhu et al [5] proposed a digital encryption technique using chaotic system based on third order level, the elevated level of security is the quality of higher order chaotic system. But they confused the encrypted image with the original image by shuffling the pixel position and changing the RGB levels of every pixel content. Kwok and Tang introduce a speedy chaotic based image encryption system with the structure of stream-cipher [6]. On the other hand, the inadequate key spaces are the foremost limitation of this technique with chaotic system.

In Marco Gortz had shown some conventional steam ciphers which could exhibit chaotic behaviors [7]. But due to the conventional cryptology, chaotic cryptography was made a better candidate than many traditional ciphers for multimedia data encryption [8]. The dissipative chaotic systems are most widely used for chaotic encryption. But the encryption based on the dissipative chaotic system [9] and conventional encryption technique has a security problem. A fractal structure which can help to predict the dynamic behavior of the chaotic carrier wave, thereby we can get a useful signal which concealed [10, 11].AS far as we attentive, there are two ideas in the literature review using the Lorentz's attractor on the basis of cryptography method. The primary one was proposed, but it is very effortless and breakable [12, 13]. In second one, Lorentz's attractor is used to efficiently generate pseudo random numbers on the basis of logistic map based ciphers [14, 15]. Thus the techniques used in this proposed system have its characteristics like sensitivity, integrity and high security. The rest of this paper is organized as follows: Section 2 the analysis of the domain is made. Section 3 deals with the system features. Section 4 gives the working principles of the system and finally in section 5 the experimental results are given.

II. OVERVIEW OF CHAOS CRYPTOGRAPHY

Over the past decade, there has been a tremendous interest are shown in studying the behavior and characteristics of chaotic system. Chaotic systems are characterized by sensitive dependence on initial conditions and similarity to random behavior.

Chaotic System	**Cryptographic Algorithms**
Phase space: Set of real numbers	Phase space: Finite set of integers numbers
Iteration	Rounds
Parameters	Key
Sensitivity to a change in initial conditions	Confusion and Diffusion
Weak security and Performance	High security and Performance

Table 1: Similarities and Difference between Chaotic Systems and Cryptographic system

Chaos has a very potential application on numerous practical blocks of a digital communication system such as compression, encryption and modulation. There are some similarities and differences between chaotic system and cryptographic algorithms which are shown in table 1. Thus the two major principles which make the cryptographic system strong is the confusion and diffusion process. Diffusion emphasis spreading out of single plaintext digits over ciphers text digits. So the original statistical structure is hided. In confusion process transformation is used to complicate the statistical structure of plain text. Hence chaos system uses cryptography to enhance the security.

III. PROPOSED ENCRYPTION SCHEME BASED ON LORENTZ, CHEN AND ROSSLER ATTRACTOR

The proposed image encryption technique based on Lorentz, Chen and Rossler chaotic attractors.

A. Lorentz Chaotic System

Lorentz chaotic system is a classical high dimensional chaotic system. This system is taken since its chaotic state is indubitable. The encrypted sequence produced by this system has three main advantages. First the structure of the system is more complex, hence it is difficult to forecast the chaotic sequences. Secondly, the real value terms of three system variables can be used separately or can be put together [16, 17]. Thirdly all the three initial conditions and control parameters can make secret key thereby allowing the secret key space of the algorithm greater than the low dimensional chaotic system. The dynamic equations of Lorentz system is given by

$$\begin{aligned} dx/dt &= \sigma (y-x) \\ dy/dt &= rx-zx-y \\ dz/dt &= xy - bz \end{aligned} \qquad (1)$$

B. Rossler System

Otto Rossler came up with a series of prototype system of ordinary differential equation in three dimensional spaces [18]. The Rossler equation is given in equation (2). This system is minimal for continuous chaos system.

$$\begin{aligned} dx/dt &= - y - z \\ dy/dt &= x + ay \\ dz/dt &= bx - cz + xz \end{aligned} \qquad (2)$$

C. Chen System

Chen found alternate traditional chaotic attractor in a easy three-dimensional independent system. Chen's systems not fit in to this general Lorenz system.

$$\begin{aligned} dx / dt &= a(y - x) \\ dy / dt &= (c - a)x - xz + cy \\ dz / dt &= xy - bz \end{aligned} \qquad (3)$$

D. Pre-Processing Method

The pretreatment or pre-processing is done by getting the rid of the integral part as real values, so that the value domain of x, y, z became as the real unified sequence value. By this way, the decimal point is moved backward for strengthening the system parameter and initial value.

$$x(i) = 10^{n} x(i) \quad round(10^{n} x(i)) \qquad (4)$$

E. Encryption and Decryption Module

First the secrete key for the image frame is generated chaotically. Fig. 1, the initial condition and the control parameter also serve to generate secrete key for the chaotic sequence. Since the chaotic sequence is unpredictable in the long run, the sequence obtained can be very well utilized to create unique key for the input image frame, thereby raising the level of security.

The value generated is added to anyone of the parameters of Lorentz, Rossler, or swig on variables and on parameter values. Finally confusion and diffusion process is done to increase the level of security. Chen chaotic system. This procedure did have a large Thus an encrypted image is obtained. Similarly the decryption fig.

2 process is also done by reversing the process of also encryption. Thus the original image is encrypted and breakable. decrypted in a high secure fashion.

The multiple stages of combined confusion and diffusion process produces a complex cipher image which is unpredictable and unbreakable. The confusion process can be done either by pixel by pixel approach or block by block approach.

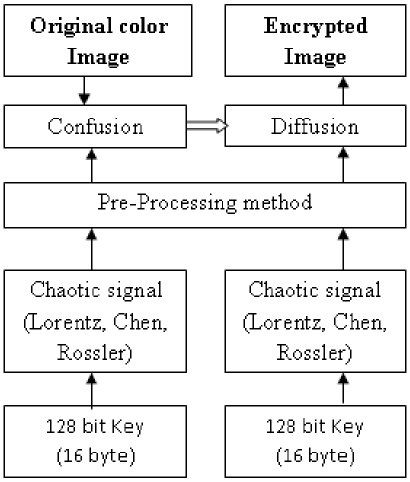
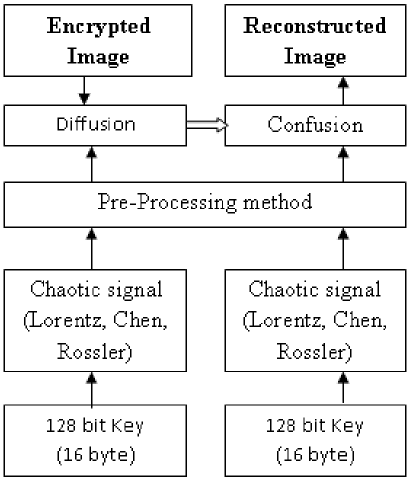


Fig 1: Encryption Process



multikey process. Single key encryption process produces complex cipher image but it is easily

Similarlily multikey image encryption proves to be secure for real time communications. The two stages of confusion and diffusion process are more attractable features of the proposed work. Many chaotic systems are available and each having its own desirable features. In the proposed work Lorentz, Rossler and Chen chaotic attractor are used for encryption and decryption phases. A 16 byte external key is used.

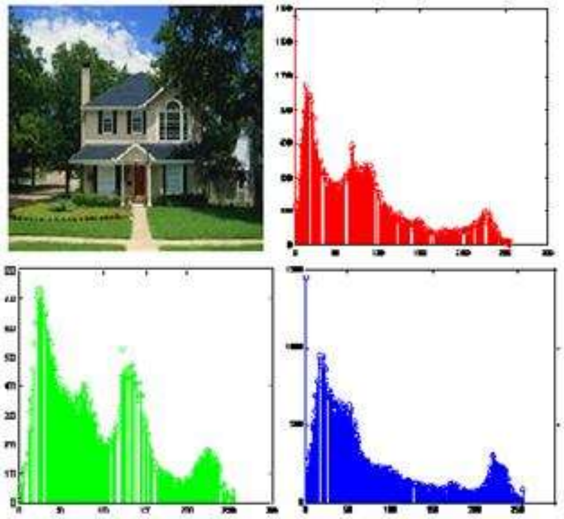


Fig 3 Original Images and its RGB Histogram

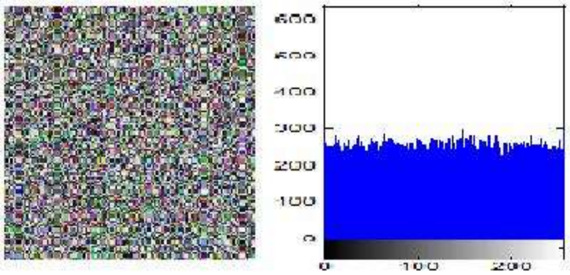


Fig 4 Encrypted Color image and its histogram using single key chaotic system

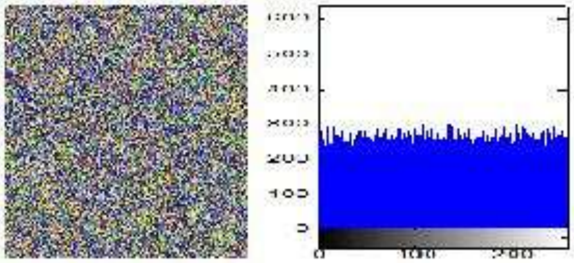


Fig 2: Decryption Process

The encryption and decryption process are carried out with single key and multi key chaotic system. In order to produce complex cipher image it is necessary to encrypt with multikey concept. The resultant image is unbreakable to any attacks.

IV. SIMULATION RESULTS AND DISCUSSION

In this paper, an empirical color image of size (256x256) is taken and shown that the proposed method has the efficient encryption performance and results in high security. Fig. 3 shows the original image and its RBG level histograms. The chaotic encryption system is well suited for grayscale and colour images. The encryption process can be done in two ways, using single key and

Fig 5 Encrypted Color image and its histogram using Multi-Key Chaotic systems

Now compare the characteristics of fig. 3 with fig. 4 and fig. 5, we can observe that the encrypted color image observed to be meaningful when compared to original image. The decryption steps are the opposite of the encryption process, therefore the decrypted image is observed with a clear and absolute without any distortion or loss. Fig. 6 shows the decrypted color image along with original is RBG histogram images.

In encryption phase, the colour image is split into red, blu and green frames. Each frames are separately encrypted with two phases, confusion and diffusion. Finally the encrypted red, blue and green frames are decrypted individually and concatenated to produce the decrypted image. The proposed work proves to be more secure for real time applications. The confusion process can also be done by block by block approach in order to reduce the encryption time.

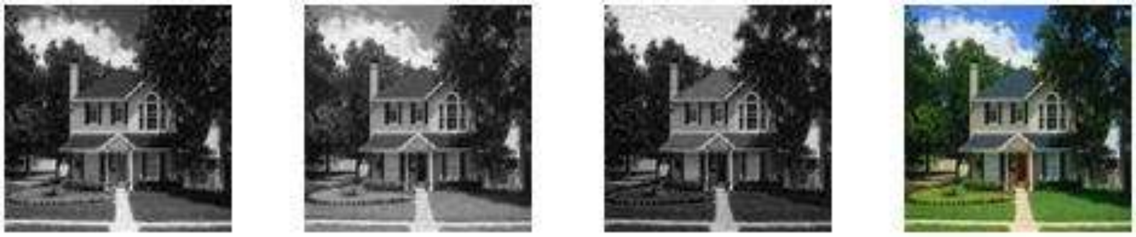


Fig 6 Decrypted Color image and its RGB frame

V. SECURITY ANALYSIS

A good encryption system needs to own outstanding sensitivity and sufficiently large key space in order to resist intruders to decrypt the original information even after large amount of time and resources. The chaotic system obtained by using Lorentz, Chen and Rossler attractor is highly sensitive to the initial values and for the parameters. It also increases the security against brute-force attack. An optimized image encryption should be sensitive for both the secret generated key. The transform of a single bit in the key should produce a completely different encryption image. Efficient key sensitivity is needed for secure image cryptosystem, which means that the encrypted image cannot be decrypted correctly even there is a small difference between the encryption and decryption keys.

VI. CONCLUSION

In this paper, a new approach for image encryption using Lorentz, Chen and Rossler attractor is proposed and its security and performance are examined in detail. The experimental outcome shows that the proposed algorithm yields high security better efficiency, image confidentiality, high encryption and decryption speed. The concept of multi-key is also proposed where the frame is encrypted by a unique key in place of changing the key for the particular frame. The key management is also inbuilt in the way the key generate. In addition it is found that the Key Space and Key Sensitivity are very high. This adopted demonstrate a very good potential in the real time application of digital color image encryption.

REFERENCES

[1] Wei Ding, Wei-qi Yan, and Dong-xu Qi, “A Novel Digital Hiding Technology Based on Tangram and Conways Game”, Proceeding of 2000 International Conference on Image Processing, Vol 1, pp. 601-604, Sept. 2000.

[2] Li Chang-Gang, Han Zheng-Zhi, and Zhang Hao-Ran, “Image Encryption Techniques: A Survey”, Journal of Computer Research And Development, Vol 39, No. 10, pp. 1317-1324, Oct. 2002.

[3] Zhao Xue-feng, “Digital Image Scrambling Based on the Baker’s Transformation”, Journal of Northwest Normal University (NaturalScience), Vol 39, No. 2, pp. 26-29, Feb. 2003.

[4] Zhu Guibin, Cao Changxiu, Hu Zhongyu, et al., “An Image Scrambling and Encryption Algorithm Based on Affine

Transformation", Journal of Computer-Aided Design & Computer Graphics, Vol15, No. 6, pp. 711-715, June. 2003.

[5] C. X. Zhu, Z. G. Chen, W. W. Ouyang, "A new image encryption algorithm based on general Chen's chaotic system," Journal of Central South University (Science and Technology) 37 (2006) 1142.

[6] H.S.Kwok, W. K. S. Tang, "A fast encryption system based on chaotic maps," Chaos Solitons Fractals 32 (2007) 1518.

[7] G. Marco, K. Kristina, and S. Wolfgang. Discrete-time chaotic encryption systems-part I: Statistical design approach. IEEE.Trans.Circuits and Systems-I, 44(10):963–970, 1997.

[8] H.Y. Ma, F. Gao and X.H. Li, Computer Engineering, 34(8), April 2008, pp.190-192.

[9] H.Dedieu, M.J. Ogorzalek, "Identifiability and identification of chaotic systems based on adaptive synchronization", IEEETrnas Circuits & SystI, 44(10), 1997, pp.948-962.

[10] R. He, P. G. Vaidya, Implementation of chaotic cryptography with chaotic synchronization,Phys. Rev. E 57, 1532 (1998).

[11] A. Ali-Pacha, N. Hadj-Said, A. M'Hamed, A. Belgoraf, Lorentz's attractor appliedto the stream cipher (ali-pacha generator), Chaos Soliton Fractals 33, 1762(2007).

[12] C. Fu, Z. Zhang and Y. Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps," Third International Conference on Natural Computation, Vol. 3, Washington, 2007, pp. 24-27.

[13] Hazem Mohammad Al-Najjar, "Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012.

[14] Hazem Mohammad Al-Najjar, Asem Mohammad Al-Najjar, "Multi- Chaotic Image Encryption Algorithm Based on one Time Pads Scheme" , International Journal of Computer Theory and Engineering, Vol.4, No. 3, June 2012

[15] Y. Cao and C. Fu." An image encryption scheme based on high dimension chaos system," Int. Cof.Intelligent computation technology and automation, 2008, pp. 104-108

[16] Fengjian Wang, Yongping Zhang and Tianjie Cao "Research of chaotic block cipher algorithm based on Logistic map", 2009 Second International Conference on Intelligent Computation Technology and Automation, 2009: 678 – 681.

[17] Wang Y, Wong KW, Liao XF, et al, "A Chaos-based Image Encryption Algorithm with Variable Control Parameters", Chaos Solitons & Fractals, vol. 41, no. 4, pp.1773-1783, 2009.

[18] Kezia.H, Sudha.G.F. "Encryption of Digital Video Based on Lorenz Chaotic System",1 6th International Conference on Advanced Computing and Communications . ADCOM.2008. Page(s): 40 - 45 IEEE Conference Publications, 200