A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images

K. Sakthidasan@Sankaran and B. V. Santhosh Krishna

Abstract—**Recent researches of image encryption algorithms have been increasingly based on chaotic systems, but the drawbacks of small key space and weak security in one-dimensional chaotic cryptosystems are obvious. This paper, a new image encryption scheme which employs one of the three dynamic chaotic systems (Lorenz or Chen or LU chaotic system selected based on 16-byte key) to shuffle the position of the image pixels (pixel position permutation) and uses another one of the same three chaotic maps to confuse the relationship between the cipher image and the plain-image (pixel value diffusion), thereby significantly increasing the resistance to attacks. The proposed system has the advantage of bigger key space, smaller iteration times and high security analysis such as key space analysis, statistical analysis and sensitivity analysis were carried out. The results demonstrate that the proposed system is highly efficient and a robust system.**

***Index Terms*—*Dynamic Chaotic system, Bigger Key Space, position ermutation,* Encryption**

I. Introduction

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Traditional image encryption [5] algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large. The chaos-based encryption[5,6] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. After Matthews proposed the chaotic encryption algorithm in 1989, increasing researches of image encryption technology are based on chaotic systems .Recently there have been many papers on chaotic encryption scheme.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications. One-dimensional chaotic system with the advantages of high-level efficiency and simplicity, such as Logistic map, has been widely used now. But their weakness, such as small key space and weak security, is also disturbing

Cryptography studies how to design good (secure and fast) encryption algorithms, and cryptanalysis tries to find security weaknesses of existing algorithms and studies whether or not they are vulnerable to some attacks. An encryption scheme is called a cipher (or a cryptosystem). The encryption and decryption procedure of a cipher is depicted in Figure 1.

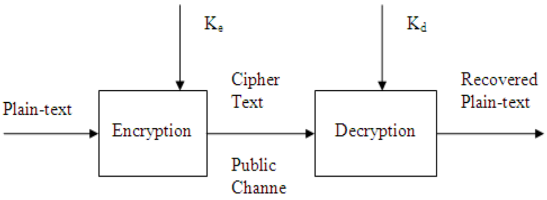

Figure 1. Encryption and Decryption procedure of a Cipher

The message for encryption is called plaintext, and the encrypted message is called cipher-text, which are denoted here by P and C, respectively. The encryption procedure of a cipher can be described as C=Eke(P), where Ke is the encryption key and E(.) is the encryption function. Similarly, the decryption procedure is P=Dkd (C), where Kd is the decryption key and D(.) is the decryption function. When Ke=Kd, the cipher is called a private-key cipher or a symmetric cipher

For private key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver via a separate secret channel. When Ke=!Kd, cipher is called a public-key cipher or an asymmetric cipher. . For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept secret, for which no additional secret channel is needed for key transfer. The cryptosystems can be classified with respect to the structure of encryption algorithm as stream ciphers and block ciphers.

Stream cipher is the method in which a key generator produces a bit stream (the Key stream) which enciphers the plain-text bit stream by simple modulo 2 additions. A stream cipher system thus hides the plain-text bit by changing the bits of it in a random way. An interceptor, who does not know the key, will not know which bits have been changed (corresponding to the occurrence of “1” in the key stream), or which ones remain unchanged (“0” in the key stream). An ideal stream cipher would use a physical (true) random number generator a Key generator. Since its output cannot be reproduced, however, decipherment would be impossible, unless the whole Key stream, with the same length as the plain-text, is transported to the legitimate receiver via a safe channel. This procedure is often impractical. Therefore mostly so-called pseudo-random number generators with special properties controlled by a relatively short Key have to be used instead as key generators.

Unlike the stream ciphers, where only one bit at a time is ciphered, whole blocks of bits are treated simultaneously. In this case the plain-text information is hidden by the fact

Manuscript received May 28, 2011.

The authors are with Electronics and Communication Engineering Department, Balaji Institute of Engineering and Technology , India.

that, depending on the key, a cipher-text block can be deciphered to any combination of plain-text bits or to as many combinations as the keys. If the keys are chosen with equal probability, then to the interceptor observing a cipher-text block, all the possible plain-text blocks are equally likely to have occurred.

Cryptography is a permanent field of interest at all time. At present secret communication plays an increasing role in many fields of common life, like banking, industry, commerce, telecommunication etc. Owing to the advance in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasing transmission ability of network gradually leads to us to acquire information directly and clearly through images. Hence, data security has become a critical and imperative issue.

Encryption is such a way that its content can be reconstructed only by a legal recipient. The technology of encryption is called cryptology. Cryptology is the branch of science dealing with the theory of secure communication algorithms. Cryptography is the process of transforming information (plain-text) into unintelligible form (cipher-text) so that it may be sent over insecure channels or it may be stored in insecure files. Cryptographic procedures, can also be used for personal identification, digital signature, access control etc..

II. Related Works

The chaos-based image cryptosystem mainly consists of two stages [2]. The plain image is given at its input. There are two stages in the chaos- based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. The pixel permutation is carried out by a chaotic system [1,2]. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers. The basic idea of encryption[5,6] is to modify the message in

In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

III. Architecture of an Chaos Based Image Cryptosystem

The chaos-based image cryptosystem mainly consists of two stages. The plain image is given at its input. The typical architecture of the chaos-based image cryptosystems is depicted in Figure 2. There are two stages in the chaos-based image cryptosystem

The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable.

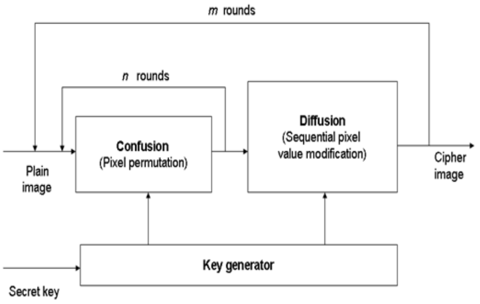

Figure 2. Architecture of proposed Chaos-based image cryptosystem

. Therefore these initial conditions and control parameters serve as the secret key. It is not very secure to have only the permutation stage since it may be broken by any attack. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image. The process of diffusion is also carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters.

In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

IV. Proposed Cryptosystem

A. Encryption System

The proposed scheme is shown in Figure 3. Different chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security.The input to the cryptosystem is the plain image which is to be encrypted. The cryptosystem consists of two stages.

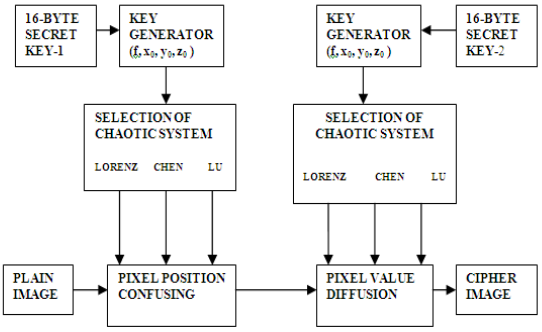

Figure 3. Architecture of proposed Chaos-based image cryptosystem

The first stage is the confusion stage and the second one is the diffusion stage. Among the three chaotic dynamic systems namely Lorenz, Chen and LU one is selected by the system parameter which is obtained from the key and it is applied to the digital color image encryption because of higher secrecy of high-dimension chaotic system.

The second step of the encryption process is to encrypt the shuffled image by changing its pixel values based on one of the three high-dimensional chaotic systems (Lorenz, Chen and LU) . This is referred to as the diffusion stage. The initial conditions and the control parameters used to generate the chaos sequence in both the stages serve as the secret key in the two stages. The resulting image is the Cipher image. Separate key is used for permutation and diffusion stages of the encryption process to improve security of the algorithm

B. Decryption System

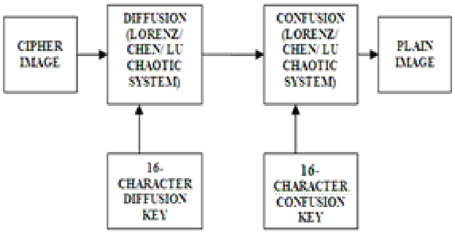
CIPHER IMAGE
DIFFUSION (LORENZ/ CHEN/ LU CHAOTIC SYSTEM)
CONFUSION (LORENZ/ CHEN/ LU CHAOTIC SYSTEM)
PLAIN IMAGE
16-CHARACTER DIFFUSION KEY
16-CHARACTER CONFUSION KEY

Figure 4. Chaos based Decryption system

The decryption system is illustrated in the Figure 4. The first stage in the decryption process is the diffused image decryption stage. In the encryption process, the pixel value diffusion was carried out with any one of the three chaotic systems. Therefore, in the decryption process to retrieve the original pixel values, again any one of the chaotic system (Lorenz, Chen, Lu) is employed in the first stage of decryption. The first stage of decryption process uses the three dimensional [8] sequence generated by any one of the chaotic system .It is a kind of high-dimensional maps and complex enough

The initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first stage. Second, in the encryption process, the pixel position permutation was carried out with any one of the chaotic system. The initial conditions and control parameters for generating the chaos-sequence were used as the confusion key. Therefore in the decryption process, the same chaotic systems with same confusion key are used to get the original position of the image. The output of the decryption system gives the original image.

V. Results and Discussion

The proposed image encryption system uses any one of the chaotic system for pixel position permutation and one of the same chaotic system for pixel value modification. Color Lena image of size 256 × 256 was taken as the test image. In Pixel position permutation stage, the Lorenz, Chen and Lu chaotic systems are used.

The original image taken for the work is given in Figure 5. The pixel position permuted image after applying one of chaotic systems such as Lorenz, Chen and Lu was obtained and shown in Figure 8. The diffused image was obtained and shown in Figure 10.

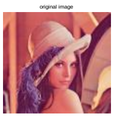

Figure 5. Original image

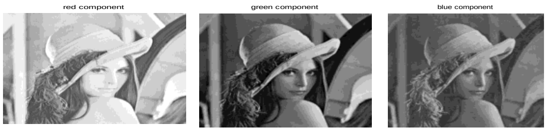

Figure 6. Separation of Red,Green and Blue component

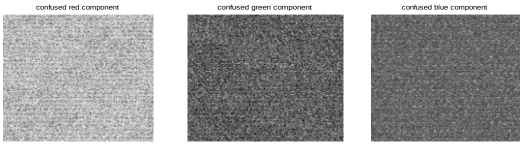

Figure 7. Confused Red,Green and Blue component

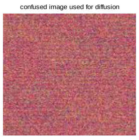

Figure 8. The Pixel Permuted image

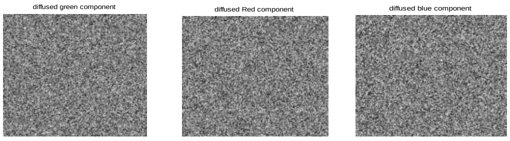

Figure 9. Diffused Red,Green and Blue component

The decryption for the encrypted image was carried out. The decrypted image after the first stage by undiffusion was obtained and shown in Figure 12.

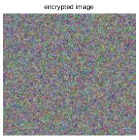

Figure 10. Encrypted image

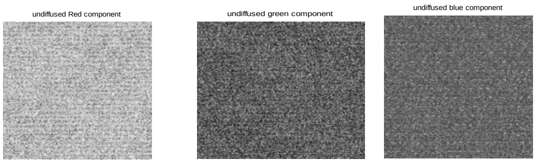

Figure 11. Undiffused Red,Green and Blue component

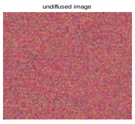

Figure 12. Undiffused image

And this will serve as the input image for the second stage of decryption. The decrypted image after applying Lorenz ,Chen and Lu chaotic systems was obtained and shown in Figure 14.

Figure 13. Unconfused Red,Green and Blue components

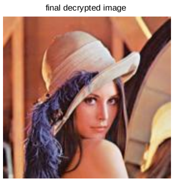

Figure 14. Decrypted image

VI. Security Analysis

To test the robustness of the proposed scheme, security analysis [12] was performed. Key space analysis, statistical analysis and sensitivity analysis were carried out to demonstrate the satisfactory security of the new scheme. The image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. It is observed that the histogram of the original image and after the confusion stage are thee same. Therefore, the diffusion function is carried out. The histogram of the final encrypted image is fairly uniform and is significantly different from that of the original image.

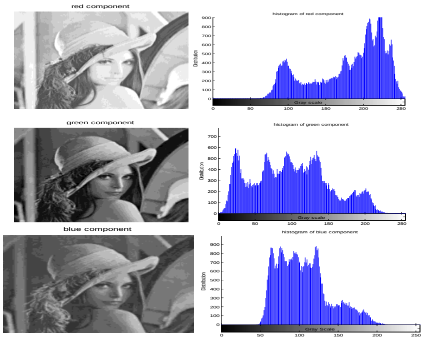

Figure 15. Histogram of Red,Green and Blue components

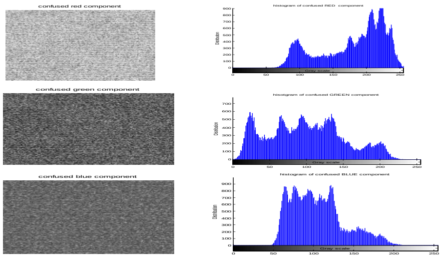

Figure 16. Histogram of confused Red,Green and Blue components

In addition to the histogram analysis the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image/cipher image are analyzed respectively. The correlation coefficient analysis indicates the relationship among pixels in the cipher image. In the new scheme the correlation among adjacent pixels is lower than that of the original image.

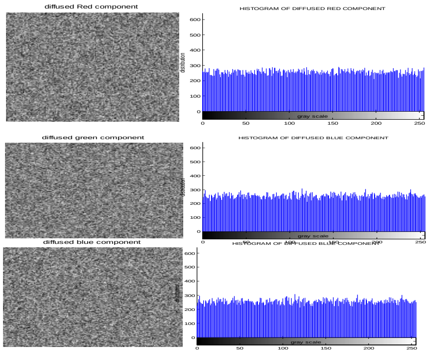

Figure 17. Histogram for diffused Red,Green and Blue component correlation coeffecient

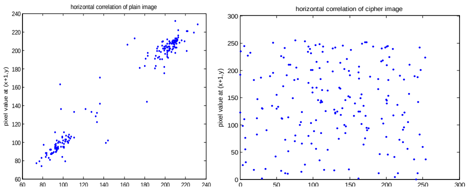

Figure 18. Horizontal correlation in a) Plane image b) Cipher imaget

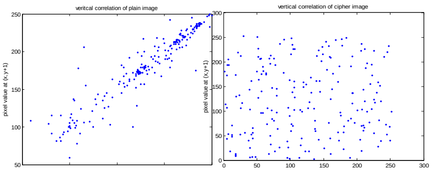

Figure 19. Vertical correlation in a) Plane image b) Cipher imaget

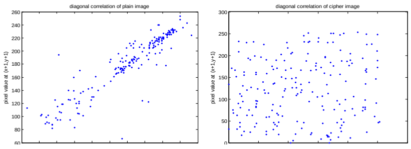

Figure 20. Diagonal correlation in a) Plane image b) Cipher imaget

TABLE I: Correlation Coefficients in Plain Image and Cipher Image

Direction of Adjacent pixels	Plainimage	Cipherimage
Horizontal	0.9791	0.0052
Vertical	0.9357	0.0539
Diagonal	0.9183	0.1141

A. *Sensitivity Analysis*

An ideal image encryption procedure should be sensitive with respect to secret key. The change of a single bit in the secret key should produce a completely different encrypted image. To prove the robustness of the proposed scheme, sensitivity analysis with respect to key is performed. High key sensitivity is required by secure image cryptosystems, which means the cipher image cannot be decrypted correctly even if there is only a small difference between the encryption and decryption keys. For testing the key sensitivity the following test is performed.

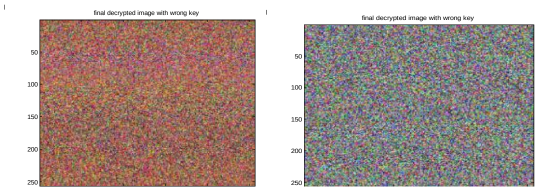

Figure 21. Image decrypted with wrong key in confusion stage

This demonstrates the high key sensitivity of the new encryption scheme. This guarantees the security of the proposed scheme against brute-force attacks to some extent

VII. Future Enhancement

Currently the chaos-based scheme was designed for still images. The chaos-based image encryption scheme can be applied to moving images as well. The prevalence of multimedia technology in the society has promoted digital images and videos to play a more significant role than the traditional texts, which demands a serious protection of users' privacy. To fulfill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties. Hence in the second phase of the paper, it is purposed to design a chaos-based image encryption scheme for moving images (videos).

VIII. Conclusion

Based on the design rules discussed earlier, the new image encryption scheme was designed. A suitable chaotic map preserving the properties of chaos after discretization was chosen. By choosing a high dimensional chaotic system, the key space is increased. Complex non-linearity was preserved by choosing suitable chaotic maps. Repeated permutations are avoided but pixel values are changed by the diffusion function. By incorporating all these features, the proposed cryptosystem avoids all the crypto graphical weaknesses of earlier chaos-based encryption systems. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the algorithm has good security and robustness.

References

[1] Xiping He Qionghua Zhang **, "**Image Encryption Based on Chaotic Modulation of Wavelet Coefficients", Congress on IEEE Image and Signal Processing (CISP'08), Sanya, Hainan, Vol.1, pp.622-626, 27-30 May 2008.

[2] Xin Zhang, Weibin Chen, "A New Chaotic Algorithm For Image Encryption", pp 889-892 IEEE ICALIP2008

[3] Dong enxeng, Chen Zengqiang, Yuan zhuzhi, Chen zaiping, "A Chaotic Images Encryption Algorithm with The Key Mixing Proportion Factor",pp 169-174 Computer Society IEEE 2008.

[4] Chong Fu, Zhen-chuan Zhang, Ying-yu Cao, "An Improved Image Encryption Algorithm Based on Chaotic Maps", Computer Society, IEEE 2007

[5] Huang Yuanshi, Xu Rongcong, Lin Weiqiang, "An Algorithm for JPEG Compressing with Chaotic Encrypting", Proceedings of the International Conference on Computer Graphics, Imaging and Visualisation (CGIV'06), 2006

[6] Peng Fei, Shui-Sheng Qui, Long Min, "An Image Encryption Algorithm based on Mixed Chaotic Dynamic Systems and External Keys", Proceedings of 2005 International Conference on Communications, Circuits and Systems,,Vol. 2, pp.1139, 27-30 May 2005.

[7] Guang ZH, Huang FJ, Guan WJ, "Chaos-based Image Encryption Algorithm", Physics Letters A, Vol.346, pp.153 – 157, 2005.

[8] Wang Ying , Zheng DeLing, Ju Lei, Wei Yaoguang, "The spatial Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceedings of the IEEE Conference on

[9] Zhang Han, Wang Xiu Feng, Li Zhao Hui, Liu Da Hai, Lin You Chou, "A New Image Encryption Algorithm Based on Chaos System", Proceedings of the 2003 IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, Changsha, China, pp.778-782, October 2003.

[10] Kristina Kelber , Wolfgang Schwarz , "General Design Rules for Chaos-Based Encryption systems", Proceedings of 2005 International Symposium on Nonlinear Theory and its Applications(NOLTA2005) Bruges, Belgium, October 18-21, pp.465-468, 2005.

[11] Yong-Hong Zhang, Bao-Sheng Kang, Xue-Feng Zhang, " Image Encryption Algorithm Based On Chaotic Sequence", Proceedings of the 16th International Conference on Artificial Reality and Telexistence - Workshops(ICAT'06),Hang Zhou, Zheijang, China, pp. 221-223, Nov.2006.

[12] Chengqing Li, "On the security of a class of Image Encryption Scheme", IACR's Crytology ePrint Archive: Report 2007/339, August 2007.

[13] Junan Lu , Xiaoqun Wu , Xiuping Han , Jinhu Lü, "Adaptive feedback synchronization of a unified chaotic system", Physics Letters A, Vol.329, pp. 327-333, 2004.

[14] Borko Furht and Darko Kirovski," Multimedia Security Handbook", CRC Press, December 2004.

K. Sakthidasan@Sankaran This Author became a Life member of ISTS, member of IACSIT and IAENG. He was born in Pondicherry on 6th October 1983. He has got his post graduate degree M.Tech –Embedded systems Technology from SRM University, Tamil Nadu, South India and Bachelors of Degree B.E – ECE from Anna University, India At present he is working as Lecturer in Electronics and Communication Engineering Department in Balaji Institute of Engineering and Technology , Chennai, Tamil Nadu, South India .Previously he as worked as Lecturer in ECE department in Mailam Engineering College for 3.3 yrs.He has published a number of papers in leading international journals and presented papers in International Conferences. His area of interest in the field of research includes Embedded Systems, Image Processing, VLSI and Network Security.

B. V. Santhosh Krishna This Author became a member of IACSIT and IAENG. He was born in Denkanikotai, Tamil Nadu on 8th September 1987. He has got his post graduate degree M.E –Communication Systems from Hindustan University, Tamil Nadu, South India and Bachelors of Degree B.E – ECE from Karunya University, India At present he is working as Lecturer in Electronics and Communication Engineering Department in Balaji Institute of Engineering and Technology , Chennai, Tamil Nadu, South India. He has published a number of papers in leading international journals and presented papers in International Conferences. His area of interest in the field of research includes Embedded Systems, Image Processing, Communication and Networking