A Novel Approach of Image Encryption and Decryption using Coupled Chaotic System

Rekha Raj, Salim Paul

Abstract*— Security is an important problem while transmitting information through an open network. Secure transmission can be done by encrypting the information. There are several methods of encryption. A novel encryption and decryption technique is discussed in this paper. Here the cryptosystem used is a coupled chaotic system in which two one dimensional chaotic maps are combined and used for encryption. A new algorithm is developed for the implementation of the coupled chaotic system. Security analysis and Statistical analysis show that this system can encrypt images effectively and can withstand several attacks like brute force attack, chosen plain-text attack etc

***Index Terms*—Cipher, Coupled chaotic system, Encryption, Decryption, Security key, Symmetric**

I. INTRODUCTION

As information technology has developed greatly, more and more information is sent over networks. While transmitting this information, security is a major problem. There is high chance of leakage of information. To avoid these problems, the information must be encrypted and then transmitted. Encryption provides security to the information which may be text, image, audio or video. Different types of encryption techniques are available depending upon the information. For example, the encryption of image is different from that of the text due to the bulk data size, correlation of pixels etc. That is why the techniques used in text encryption are not suitable for image encryption. Image is digital information and there are several methods for image encryption. Encryption algorithms can be mainly classified into two groups, Public Key Algorithm and Private Key algorithm.

A. Public Key Algorithm

This is an asymmetric algorithm in which two keys are used. One is public key and other is private key. In this algorithm the message can be encrypted using the public key which is known to everyone and can be decrypted using the private key or the secret key known only to the receiver.

B. Private Key Algorithm

This is a symmetric algorithm where only one key is used, Private Key. Here same key is used for encryption and decryption ie, the private key. It is known only to the transmitter and the receiver. This algorithm uses either stream ciphers or block ciphers.

A wide variety of image encryption algorithms are there. Among them chaotic image encryption is more trustworthy. A novel method of encryption by combination of two one-dimensional chaotic maps, about its performance, speed, security etc are discussed here.

II. CHAOTIC SYSTEM OF IMAGE ENCRYPTION

The chaotic system of image encryption [1] is one of the most efficient methods of image encryption. It has certain special properties like sensitivity to initial conditions and control parameters, randomness, non-convergence etc. The chaotic maps are used for encryption in chaotic systems. There are mainly two types of chaotic maps—one dimensional and multi-dimensional chaotic maps.

Multi-dimensional chaotic maps[2] have many applications in image security. But they have complex structure and multiple parameters and so they are difficult to implement. One dimensional chaotic maps are simple and can be implemented easily. But they have smaller chaotic ranges and chaotic sequences are non-uniformly distributed in the chaotic range. Both methods have advantages and disadvantages. A better method can be implemented using the combination of two one dimension methods, a combinational chaotic system. The figure of a typical chaos based image encryption system is shown below.

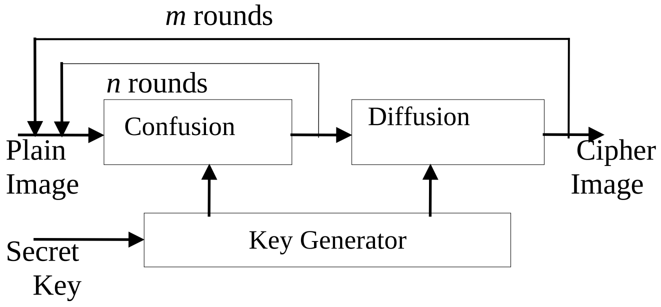


Fig.1 A typical chaos-based image cryptosystem

A. Combinational Chaotic System

In this system two 1D chaotic maps are combined and a new chaotic system is formed. In the new system, the chaotic range can be extended and have a wide range of parameter settings. Here the chaotic sequence can be uniformly distributed within the chaotic range. This system provides better encryption.

The application of this system can be demonstrated by a new algorithm which provides better security to the data by the better confusion and diffusion properties[3]. Various attacks like brute force attack, chosen plain attack etc can be withstand using this method.

Manuscript published on 30 June 2016.
***** Correspondence Author (s)

Rekha Raj, Department of Electronics & Communication, SCT College of Engineering, Pappanamcode, Thiruvananthapuram (Kerala). India.

Salim Paul, Department of Electronics and Communication, SCT College of Engineering, Pappanamcode, Thiruvananthapuram (Kerala). India.

One of the main advantages of this method is whenever an image is encrypted by this algorithm, each time a different encrypted image is obtained. This property of the system helps us to withstand chosen plain text attack.

The new system is a nonlinear combination of two different one-dimensional chaotic maps and can be defined as

$$X_k+1=(A(u, X_k)+B(v, X_k)) \bmod 1 \qquad (1)$$

where $A(u,X_k)$ and $B(v,X_k)$ are two 1D chaotic maps with parameters u and v, mod is the modulo operation and k is the number of iterations.

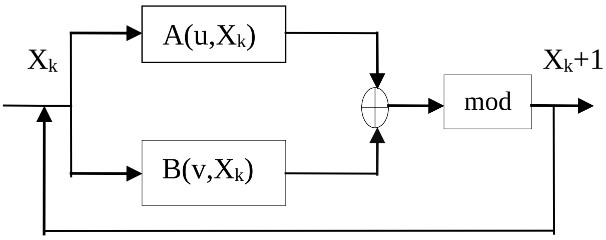


Fig.2 Combinational Chaotic System

B. Logistic-Tent System

The new chaotic system used here is Logistic-Tent System which provides mixed chaotic property since it is a combination of two chaotic maps. It exhibits better performance and even one of the chaotic maps is out of range. Here the one dimensional chaotic maps[4] used are Logistic map and Tent map. The new chaotic system is Logistic-Tent system. In the new system the parameter settings of the chaotic maps are also combined. The logistic tent system can be defined as

$$\begin{aligned} X_k+1 &= (L(n,X_k)+T((4-n),X_k)) \bmod 1 \\ &= (nX_k(1-X_k)+(4-n)X_k/2)) \bmod 1 \qquad X_i < 0.5 \\ &= (nX_k(1-X_k)+(4-n)(1-X_k)/2\ ) \bmod 1 \qquad X_i \geq 0.5 \end{aligned} \qquad (2)$$

where parameter n ϵ (0,4]. This system provides better performance within the chaotic range (0,4]. The chaotic range of this system is larger compared to its seed maps, logistic map and tent map. The output sequence is uniformly distributed within [0,1]. The density function is also uniformly distributed.

III. ENCRYPTION

The application of the Logistic-Tent chaotic system can be demonstrated using a new encryption algorithm. The encryption stage consists of four rounds. Each round includes different steps like Random pixel Insertion, Substitution, and Image Rotation.

A. Algorithm

- A random pixel is inserted at the beginning of each row of the original image.
- Apply a substitution process to change the data values in the matrix. The substitution process is done by performing bit level XOR operation of the random sequence generated by the LTS system and the random pixel inserted image.
- After substitution, remove the first pixel from each row of the resulting image matrix.
- Rotate the matrix 90^0 counter clock wise
- The encrypted image is obtained by repeating the above processes four times.
- After first round of encryption, the encrypted image is feed back to the input of the random pixel insertion process.
- Repeat the process three times and after the fourth round, the resulting image is the final encrypted image.

This algorithm has the ability to convert plain image into noise like image with excellent confusion and diffusion. The algorithm consists of security keys having six portions: the LTS parameter (n_0), initial value, and LTS parameters in each round (n_1 ,n_2 ,$n_3,$ n_4). The initial parameter and the control parameters can be defined by the users. The encryption procedure can be described using the block diagram shown below.

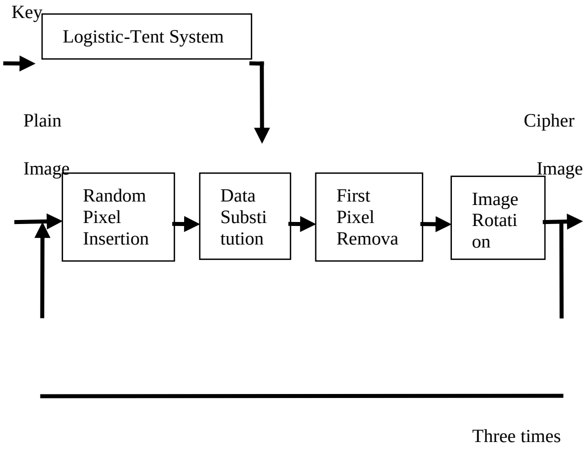


Fig.3. Image Encryption Algorithm

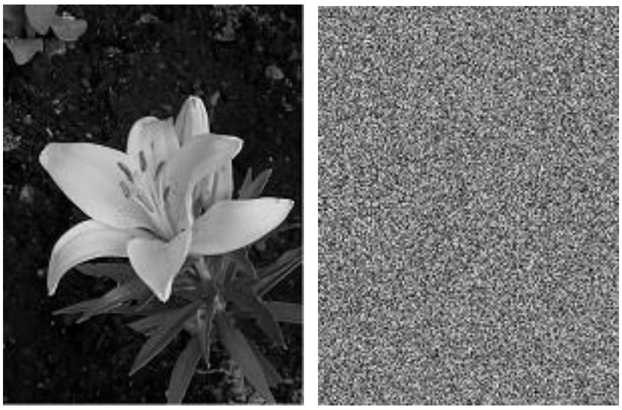


Fig.4.(a) Original Image (b) Cipher Image

IV. ADVANTAGES

- Every time the algorithm is applied to the same image with same security keys, a completely different encrypted image can be obtained.
- A fast encryption is done due to the parallel implementation of the Substitution process.
- The encrypted images have a high level of security, since the encrypted image possesses excellent confusion and diffusion properties.
- The encrypted image can withstand several attacks like chosen-plaintext attack, data loss and noise attack

V. DECRYPTION

In image decryption, the encrypted image is decrypted using the inverse procedures of encryption. The cipher image is rotated 90^0 clock wise and the rotated image is inserted with random pixel vector.

Decryption is done by inverse substitution process and then the first pixel is removed. These steps are done three times repeatedly and finally the decrypted image is obtained.

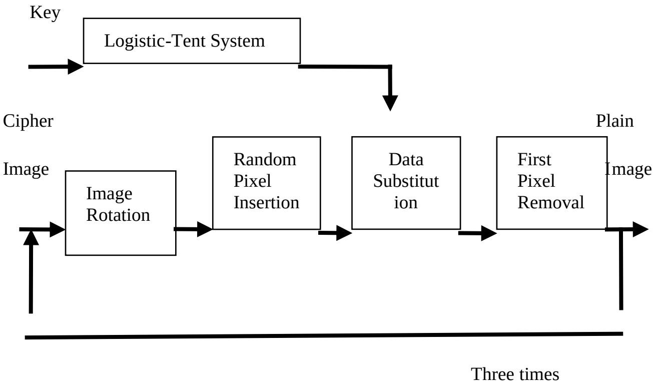


Fig.5. Image Decryption Algorithm

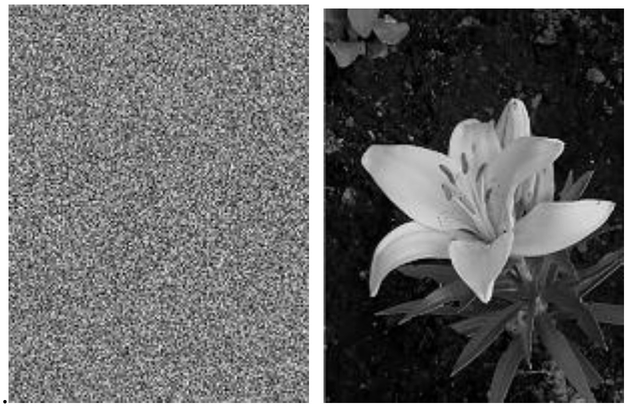


Fig.6 (a) Cipher Image (b) Decrypted Image

VI. SECURITY ANALYSIS

Security is the major consideration of an encryption algorithm. Security key analysis [6] includes key space analysis and key sensitivity analysis.

A. Security key Analysis

Key Space: It is the set of all possible keys that can be used to generate a key. In this algorithm, five control parameters and one initial parameter are used as keys. The parameters r_0, r_1, r_2, r_3, r_4 used here are in the range [0,4] and the initial parameter $S_1(0,0)$ ϵ [0,1]. The length of each parameter determines the key space. The length of the parameter can be increased so as to resist the brute force attack.

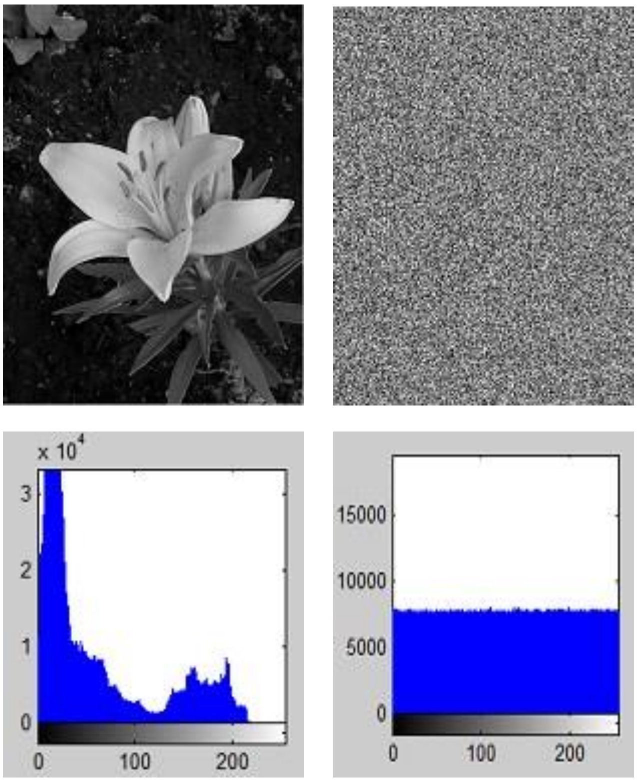
Key Sensitivity: When a small change is applied to any one of the control parameters keeping others unchanged, it will result a change in the encrypted image. That is, a small change in any one of the control parameters results in a change in the encrypted image. This can be known from the pixel to pixel difference of the encrypted image. Similarly, the decryption process also needs correct key to decrypt the encrypted image. A small change in the key cannot provide the decryption of the encrypted image.

VII. STATISTICAL ANALYSIS

The encrypted images can be successfully analyzed using statistical analysis. It includes histogram analysis, correlation analysis and Information Entropy.

A. Histogram

Histogram shows how pixels are distributed in the original image [5] by graphing the number of pixels at each gray level. Histograms of original image and plain image are shown below. The histogram of the original image shows large spikes correspond to different gray scale values. The histogram of the encrypted image shows a uniform distribution and thus it does not provide any clue for statistical attack.



(a) (b)

Fig.7 (a) Encrypted image and its histogram (b) Decrypted image and its histogram

B. Correlation Analysis

Normally, the pixels of an image are highly correlated with its adjacent pixels either in horizontal, vertical and diagonal direction. In the cipher image, there is no correlation[7] between the adjacent pixels. The correlation coefficient can be calculated using the formula

$$Cxy=(E[(x-\mu x)(y-\mu y)])/(\sigma x\ \sigma y) \qquad (3)$$

where μ and σ are the mean value and standard deviation respectively. E[.] is the expectation value. For better encryption, the cipher image has correlation values close to zero. Table 1 compares the correlation of original image[9] and the encrypted images obtained using new chaotic system and AES algorithm.

C. Information Entropy

It is a concept that helps to evaluate the uncertainty in a random variable or evaluating the randomness of an image. A large Information Entropy (IFE) value implies the excellent encryption. The maximum value of IFE of a gray scale image is 8. Compared with AES algorithm[8], the IFE value of the new chaotic system is slightly higher and this shows a better level of encryption. The table 2 shows the IFE scores of images after and before encryption using the two different algorithms.

Table 1. Correlation values

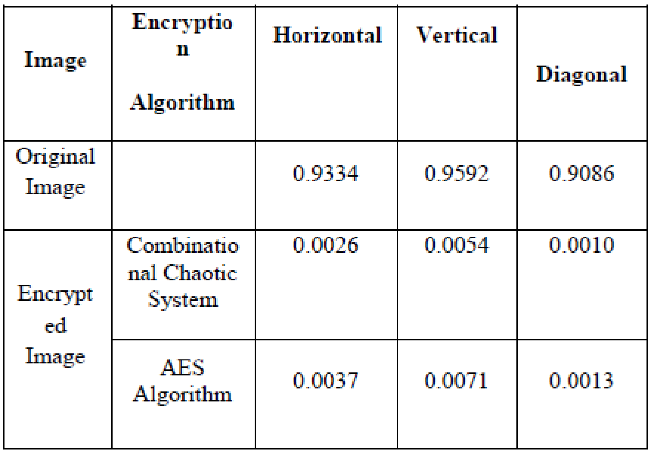


Image	Encryption Algorithm	Horizontal	Vertical	Diagonal
Original Image		0.9334	0.9592	0.9086
Encrypted Image	Combinational Chaotic System	0.0026	0.0054	0.0010
	AES Algorithm	0.0037	0.0071	0.0013

Table 2. Information Entropy Analysis

Image	Encryption Algorithm	Entropy Values
Original Image		7.009
Encrypted Image	(a) Combinational chaotic system	7.999
	(b) AES System	7.996

VIII. SPEED ANALYSIS

While comparing the encryption speed of two different algorithms, the new chaotic system and the AES [10] algorithm, the chaotic system shows better performance than the AES algorithm. The encryption time of the chaotic system is 2.49 seconds and that of the AES algorithm is 756.72 seconds.

IX. CONCLUSION

A new chaotic system which is a combination of two one dimensional chaotic systems is used for image encryption. The application of this chaotic system can be implemented using a new encryption algorithm. Image encryption and decryption can be done using this algorithm. The encrypted images have excellent confusion and diffusion properties compared to other algorithms. The encrypted images can withstand several attacks like brute force attack, chosen plain text attack, data loss and noise attack. Security and Statistical analysis of the algorithm is done and compared it with the AES encryption algorithm. Results show the better performance of the new combinational chaotic system.

REFERENCES

1. Yicong Zhou, Long Bao and C.L.Philip Chen"A New 1D Chaotic System for Image Encryption", Signal Process. 97(2014) pp.172-182.
2. Kanso and M. Ghebleh "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map,"Commun Nonlinear SciNumerSimulat17 (2012) pp.2943–2959
3. G.A.Sathishkumar ,Dr.K.Bhoopathy bagan and Dr.N.Sriraam "Image Encryption Based on Diffusion and Multiple Chaotic Maps" ,International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March2011,pp.181-194
4. Shoaib Ansari, Neelesh Gupta and Sudhir Agrawal, "An Image Encryption Approach Using Chaotic Map in Frequency Domain" ,International journal of Emerging Technology and Advanced Engineering-Volume 2, Issue 8,
5. Gururaj Hanchinamani and Linganagouda Kulakarni, "Image Encryption Based on 2-DZaslavskii Chaotic Map and Pseudo Hadmard Transform", International Journal of Hybrid Information Technology Vol.7, No.4 (2014),pp.185-200.
6. Xiaoling Huang,Guodong Ye, and Kwok-Wo Wong, "Chaotic Image Encryption Algorithm Based on Circulant Operation", Abstract and Applied Analysis,Volume2013
7. Xianhan Zhang and Yang Cao, "A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme", The Scientific World Journal Volume 2014(2014).A. E. Rohlem S, Elagooz, and H. Dahshan, "A novel approach for
8. designing the s-box of advanced encryption standard algorithm (AES) using chaotic map", IEEE Conference Publications 2005,pp.455-464
9. Fu C1, Chen JJ, Zou H, Meng WH, Zhan YF and Yu YW, "A chaos based digital image encryption scheme with an improved diffusion strategy", Opt Express 2012, 20(3),pp.2363-78
10. Dr. Prerna Mahajan and Abhishek Sachdeva, "A Study of Encryption Algorithms Aes, Des and Rsa for Security", Global Journal of Computer Science and Technology Network, Web and Security 2013,Volume.13, Issue15, pp.15-22