International Journal For Technological Research In Engineering
Volume 3, Issue 10, June-2016 *ISSN (Online): 2347 - 4718*

CHAOS BASED PARTIAL ENCRYPTION OF GRAYSCALE IMAGE USING COUPLE TENT MAP BASED ON PSEUDO RANDOM NUMBER GENERATOR

Meghana H K[1], Prabhavathi K[2]
[1]PG Scholar, VLSI Design & Embedded System, [2]Asst. Professor, Department of ECE
BGS Institute of Technology, BG Nagar, Mandya, Karnataka, INDIA

ABSTRACT: Chaos based Image encryption plays a very important role in Cryptographic work. The important properties of chaos are good cipher confusion and cipher diffusion. The proposed system mainly deals with Chaos based Partial Encryption for grayscale Images. Speed and time are the most important factor in partial encryption. The procedure for partial encryption of grayscale image has been explained. The original grayscale image are decomposed into corresponding binary eight bit planes then the decomposed bit planes are encrypted using couple tent map method based on pseudo random number generator (PRNG). The four significant bit planes are measured by the contribution of a bit plane. These bit planes are encrypted which are obtained by using one of the relation called tent map based pseudorandom binary number generator. After tent map method, the insignificant bit planes are combined with encrypted bit planes to get the final encrypted image. Then we should evaluate the performance of proposed scheme. The security tests are used for security measurements and effectiveness of the proposed algorithms. Many tests were conducted which includes visual test, histogram analysis, key space test, entropy test and also we can measure the Encryption quality. Finally we will get a latest cipher which has proper security and efficient.

Keyword: Chaos, Couple tent map, Cryptography, Pseudorandom binary number generator.

I. INTRODUCTION

Security of images becomes an important subject in real world communication. Encryption is a significant method for securing data in open network. During transmission, by using encryption technique we can prevent our information from illegal access. There are so many customs to pass data through internet like e-mail etc. Images are broadly used in real world communication. The major trouble with transferring message through the open network is the authenticity. Security of data means protecting the information from criminal use. The chaos based encryption is important and it will suggest an efficient way. The Chaos type encryption scheme deals with problems of highly secure encryption of images. There are distinct properties with respect to chaos like randomness, sensitivity on initial conditions, other system parameters, etc. Chaos is the advanced characteristic which is related to nonlinear dynamic system. Chaos deals with definite principles of system values. The Chaotic characteristics of a non linear system will apparently look random. In real world, the existing techniques will consume high computational time for the encryption process. An image is a combination of both significant and insignificant data but some part of the information will be present in the significant part. Hence it is enough to encrypt the significant bit planes. No need of encrypting the complete image plane. It is enough to encrypt the significant part in order to speed up the complete process of encryption. In the proposed scheme partial encryption technique [1]-[9] is used. In partially encrypting scheme, only the significant data will be encrypted leaving the insignificant data. Here we will get the fast and safe algorithm for partial encryption of image by using the chaotic functions.

II. METHOD DECRIPTION

A. Bit Plane Decomposition

Image encryption plays an important role in information security criteria. Image encryption process is used to convert the plain image into cipher image. Bit plane slicing [10] is done to give security to the image. The aim of Bit plane slicing is done to decompose the original image into eight bit. Then the bit plane will be rotated to offer improved encrypted image. It will do hacking procedure much complicated. It mainly deals with two schemes, namely bit plane slicing and image rotary motion in order to get proficient image encryption. To know the importance of each bit in an image bit plane slicing method is used. Encryption is the method of transferring message in a safe manner. Before transmitting, it scrambles the image to modify the configuration of a grayscale image. Hence the aggressor cannot hack the image since it is hard for attacker to get the plain grayscale image. The main criterion is to give enhanced security to original image. The pixel value of image will depends on scrambling of image. In order to analyze the importance of each bit in an image, the digital image is divided into 8 bit planes. The small change in the color of an image will affect the bit rate of image. The color image will have so many pixels. It will be divided into 8 bit planes. It is essential to characterize the higher and lower order bits to know the significance of every bit in image. It gives enhanced image encryption and in this process the overall image quality will not be changed.

B. Chaos Based Pseudo Random Number Generator

Encryption process takes place in two different modes such as confusion and diffusion. These different modes will

provide more security in an efficient way. The grayscale image will be taken as its input. In the confusion phase, the pixel incarnation will be done and in the entire image the position of the pixels will be scrambled. It will not disturb the value of the pixels and we can see the unrecognizable image. Hence the control parameters and initial conditions will be served as top secret key. It is not good to have permutation phase [11] because this phase perhaps broken down by aggressor. In order to get better security of the image, diffusion process will be adopted. Here in the whole image, the value of each pixel will be changed. The diffusion process is done through a chaotic tent map but it is reliant on the control parameters. The pixel values are customized by the sequence generated from one of the frenzied systems with the help of external key. To get the level of security, the whole confusion and dissemination process repeats for a numerous times. In the Chaotic maps, the randomness property is more suitable for encrypting image. The random sequence is generated by using below equations,

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu_2 x_n \text{ for } x_n < \frac{1}{2} \\ \mu_2(1 - x_n) \text{ for } \frac{1}{2} \le x_n \end{cases} \quad (1)$$

$$y_{n+1} = f_\mu(y_n) = \begin{cases} \mu_2 y_n \text{ for } y_n < \frac{1}{2} \\ \mu_2(1 - y_n) \text{ for } \frac{1}{2} \le y_n \end{cases} \quad (2)$$

By comparing the outputs of both the tent maps, the bit sequence is generated.

$$g(x_{n+1}, y_{n+1}) = \begin{cases} 1 & \text{If } x_{n+1} > y_{n+1} \\ 0 & \text{If } x_{n+1} \le y_{n+1} \end{cases} \quad (3)$$

III. PROPOSED SCHEME

A. Encryption Method

A partial encryption process is derived from the information separation as perception based insensitive and sensitive data. The partial image encryption process will be shown in figure 1. The grayscale image will be taken as input and it is divided into 8 bit planes then major bit planes are determined. A key is generated for the significant bit and is encrypted. The combination of encrypted significant bit and insignificant unencrypted bit gives the encrypted gray-scale image. Couple tent map based pseudorandom binary number generator method [12] is used for encryption process.

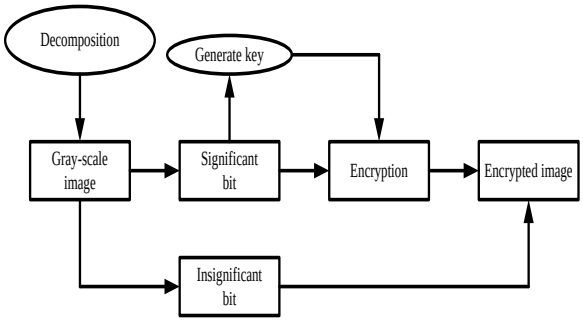

Figure 1: Image encryption process

Encryption steps are explained below,

Step 1: Assume $I_{original}$ (x, y) be the plain image of range M × N where 'x' range from 0 to M - 1 and 'y' ranges from 0 to N - 1.

Step 2: In a plain image, each pixel value $P_i(x, y)$ will be divided into equivalent eight bit binary plane. Hence 8 bit planes are produced.

Step 3: Major bit planes will be calculated by level α critical region from the hypothesis H_0 where H_0 is the i^{th} bit plane is significant against the alternative hypothesis and $H_1$is the i^{th} bit plane is not significant bit planes.

Step 4: Major keys are used for diffusing the major bit planes by using the method called Couple tent map which is based Pseudo random binary number generator by triplet (x_0, y_0, μ) values.

Step 5: The significant bit planes are ciphered and are determined by α% level of significance.

Step 6: The mixture of major encrypted bit planes and unencrypted bit planes gives the encrypted image.

B. Decryption Method

The image decryption for the grayscale image is shown in figure 2. An encrypted grayscale image will be divided into eight bit plane, and the major bits will be determined. The generated key in the encryption process is used for a decryption process. The combination of decrypted significant bit and insignificant bit gives the original gray-scale image.

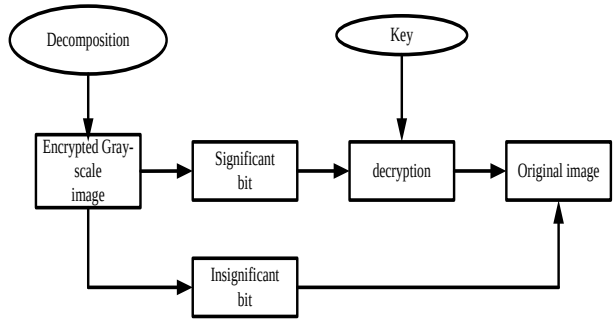

Figure 2: Image decryption process

Decryption steps are explained below,

Step 1: Assume I_{Cipher} (x, y) be the cipher image of range M × N where 'x' range from 0 to M - 1 and 'y' ranges from 0 to N - 1.

Step 2: Each pixel value $P_i(x, y)$ of the cipher image that is I_{Cipher} (x, y) will be divided into its resultant 8 bit binary planes.

Step 3: Major bit planes will be analyzed by the level α critical region from the hypothesis.

Step 4: After receiving the triplet (x_0, y_0, μ) keys for diffusion process, the major bit planes will be produced using Couple map based on Pseudo random binary number generator.

Step 5: Then the significant cipher bit planes will be deciphered and are determined by α% level of significance.

Step 6: The decipher bit planes and the insignificant bit planes are combined together to form original Image.

IV. STATISTICAL TEST AND ANALYSIS

By using statistical analysis image cipher can be successfully crypt analyzed. In order to see the stiffness of Chaos based algorithm [13], statistical tests were conducted which performs some important properties. This algorithm will also helps in resisting the nature against statistical attacks. So many analyses like histogram analysis, correlation test, key

space analysis, key sensitivity test and entropy test has been conducted.

A. Histogram Analysis

The histogram of the image is the study of allotment of pixels in an image and it will be demonstrated by plotting graph between number of pixels and intensity level. The pixels should be distributed uniformly against the intensity values to get a perfect encrypted grayscale image.

B. Correlation Coefficient Analysis

The measure of correlation is called correlation coefficient. The range of correlation coefficient is given by ($-1 \leq r \geq +1$). The correlation analysis helps us to know the grade and route of the correlation among 2 variables. Correlation is an arithmetical instrument helps to compute and investigate the degree of correlation among 2 variables. Correlation gives the relationship among variables for correlating two incidents or events. The correlation coefficient [14] for horizontal and vertical pixels are calculated from the below equations,

$$r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} \text{ where } cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y}) \quad (4)$$

$$\sigma_x = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2 \text{ and } \sigma_y = \frac{1}{n}\sum_{i=1}^{n}(y_i - \bar{y})^2 \text{ with} \sigma_x \neq 0 \text{ and } \sigma_y \neq 0 \quad (5)$$

C. Key Sensitivity Test

A good cryptosystem must be susceptible for minute variation in secret key. During Encryption scheme if there is any change in secret key, then we will get a fully dissimilar encrypted grayscale image. The Chaos based partial encryption scheme will be susceptible to a minute alteration among the secret key. The partial image encryption scheme must be sensitive to top secret key. In order to see the bulkiness of chaos based partial encryption system, sensitivity analysis with respect to key should be done. To get highly secure image, then Cryptosystems with high key sensitivity is required. IF we see any dissimilarity between the encryption and decryption keys the cipher image would not be decrypted properly.

D. Key Space Analysis

The analysis result shows that Chaos based partial Encryption system is extremely perceptive to the secret key. During the Decryption process if the decryption key changes, then we can see a great change among decrypted image and the plain image. The key used during the image cipher can be of any size. If we use larger key then the encryption speed will be reduced and larger key are not used during image transmission. If we choose small sized secret key then Cryptanalysis [15] can be done in easy manner. The total number of dissimilar keys used during the Cryptanalysis will define the key space. It can be used as the control parameters in the encryption technique. A good encryption method should have a huge key space to oppose all types of beast strength attack.

E. Measurement Of Encryption Quality – MSE, PSNR, NPCR, UACI.

The measure of encryption quality can be articulated as the digression among the original image and the encrypted image. The feature of image encryption can be described below. Mean square error is the part of digital image processing technique to find the errors. Two MSE values are taken and evaluated then compared with each other to find the accuracy of a digital image. MSE is extensively used to calculate the level of image deformation since it can characterize the entire gray value error present in whole grayscale image. Peak signal to noise ratio is the ratio among the highest probable power of a signal and power of the humiliating noise that can affects the reliability of depiction. PSNR is known for calculating the superiority of restoration of lossy type compression. NPCR is defined as the quantity of pixels change rate of encrypted image whereas single pixel of plain image will be altered. It mainly focuses on the complete quantity of pixels which changes value in discrepancy attacks. NPCR is used to compute the compassion of the algorithm to negligible changes in the original grayscale image. UACI stands for unified average changing intensity. It calculates the typical intensity of distinction among the plain grayscale image and the cipher image. UACI is used to enumerate the differentiation among the encrypted image and equivalent plain image.

Let C(i, j) where i = 0,1,2,3 … , M - 1 and j = 0,1,2,3 … , N – 1 be the gray level of the pixels of a cipher image and P(i, j) be the gray level of the pixels of a original image. The mean square error between these two images can be calculated by,

$$\text{MSE} = \frac{1}{\text{M} \times \text{N}} \sum_{\text{i}=0}^{\text{M}-1} \sum_{\text{j}=0}^{\text{N}-1} |\, \text{C(i,j)} - \text{P(i,j)}|^2 \quad (6)$$

$$\text{PSNR} = 20 \times \log_{10}\left(\frac{255}{\sqrt{\text{MSE}}}\right) \quad (7)$$

Two cipher images, $C_1(i, j)$ and $C_2(i, j)$ where i = 0,1,2,3 …. , M - 1 and j = 0,1,2,3 .... , N – 1 are taken in order to evaluate the number of pixel change rate.

$$\text{NPCR} = \frac{\sum_{\text{i,j}} \text{D(i,j)}}{\text{M} \times \text{N}} \quad (8)$$

$$where D(i,j) = \begin{cases} 0, if C_1(i,j) = C_2(i,j) \\ 1, if C_1(i,j) \neq C_2(i,j) \end{cases}$$

$$UACI = \frac{1}{M \times N}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (9)$$

V. EXPERIMENTAL RESULTS

Four images like backbone, brain, boat and baboon grayscale images are taken as input. For the given input, respective outputs like histogram analysis and correlation analysis for both plain and cipher images are revealed below.

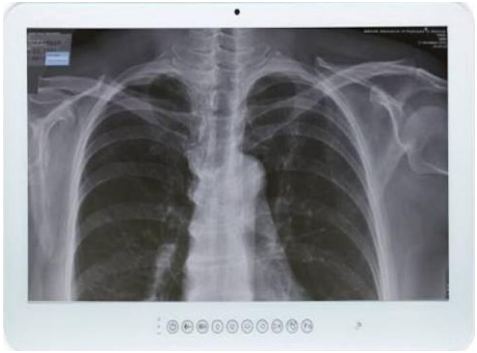

Figure 3: Original grayscale image of backbone

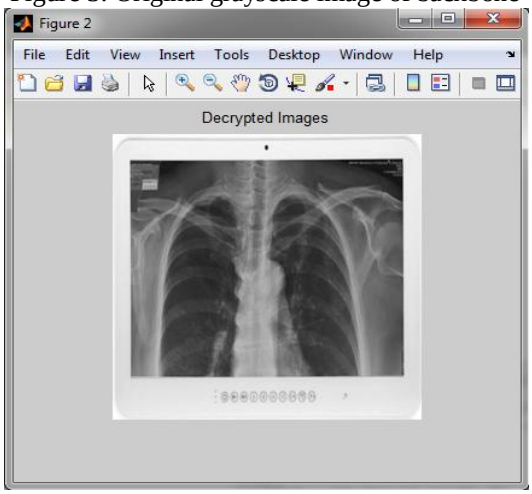

Figure 4: Cipher image of backbone

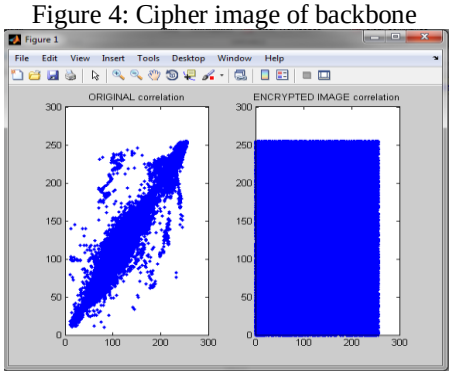

Figure 5: Correlation of original and encrypted grayscale images

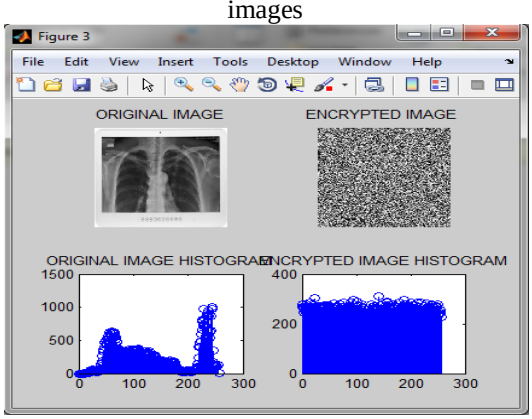

Figure 6: Histogram analysis of original and encrypted grayscale images

Table 1. Correlation coefficient analysis between the original image and encrypted image

Name of the image	Horizontal pixels of plain image	Horizontal pixels of cipher image	Vertical pixels of plain image	Vertical pixels of cipher image	Correlation b/w pixels of plain image & cipher image
Backbone	0.6202	0.0075	0.7487	0.1160	-0.0068
Brain	0.9990	-0.1065	0.7844	-0.0042	0.0026
Boat	0.9787	0.0064	0.8000	-0.0054	-0.0017
Baboon	0.8891	-0.0777	0.4421	0.0236	-0.0099

Table 2. Measurement of Encryption quality and Time comparison of Encryption and Decryption

Name of the image	MSE	PSNR	UPCR	UACI	Encryption time (in Second)	Decryption time (in Second)
Backbone	1.0784e+04	7.8032	97	19 %	0.8563	0.2755
Brain	1.2556e+04	7.1423	99	26 %	0.9098	0.2840
Boat	7.5283e+03	9.3276	99	19 %	0.9976	0.3082
Baboon	6.8648e+03	9.7645	99	19 %	0.9190	0.3369

Table 1 represents the correlation coefficient analysis among the original image and encrypted image. Table 2 gives the measurement of Encryption quality and also time comparison among Encryption and Decryption.

VI. CONCLUSION

The proposed scheme deals with partial encryption and decryption of grayscale images by using couple tent map method based on Chaos. In this proposed algorithm only the significant bit planes are determined to encrypt the image. By using the generated key stream significant bit planes are encrypted on the basis of a chaos based pseudorandom binary number generator technique. The insignificant bit planes are left in order to consume time. In partial

Encryption, speed and time are very important. The simulation experimental results prove that the encryption algorithm is effective and simple to realize.

REFERENCES

[1] N. Pisarchik, N. J. Flores-Carmona, M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices", CHAOS Journal, American Institute of Physics, vol. 16, 2006.
[2] C. Dongming, Z. Zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists, 2008.
[3] N. K. Pareek, V. Patidar, K. K. Sud, " Encryption image using chaotic logistic map." Image and Vision Computing, vol.24, no.9, pp. 926–934, 2006.
[4] N.K. Pareek, Vinod Patidar, K.K. Sud, "Cryptography using Multiple one-dimensional chaotic maps", Communications in Nonlinear Science and Numerical Simulation, 2005.
[5] N.K. Pareek., Vinod Patidar., K.K. Sud, "Image Encryption and Decryption using chaotic logistic map", Image and Vision Computing, 2006.
[6] Shubo Liu, Jing Sun, ZhengquanXu, "An Improved Image Encryption Algorithm based on Chaotic System" , Journal of Computers, vol. 4, no. 11 (2009).
[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps." International Journal of Bifurcation and Chaos, vol.8, no.6, pp.1259-1284, 1998.
[8] S. Som, A. Kotal, "Confusion and diffusion of grayscale images using multiple chaotic maps," in Proc. NCCCS 2012, Durgapur, Dr. B. C. Roy Engineering College.
[9] H. T. Panduranga, S. K. Naveen Kumar, "Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique", International Journal of Computer Applications (0975 – 8887) ,vol. 60 no.16, December 2012.
[10] A. Razzaque, Dr.N.V.Thakur, "An Approach to Image Compression with Partial Encryption without sharing the Secret Key", IJCSNS International Journal of Computer Science and Network Security, vol. 12 no.7, July 2012.
[11] B. D. Parameshachari, Dr. K M S Soyjaudah, "A Study of Binary Image Encryption Using Partial Image Encryption Technique", International Journal of Modern Engineering Research (IJMER), vol.2, Issue.3, pp. 955-959, ISSN: 2249-6645, May-June 2012.
[12] B. D. Parameshachari, K M Sunjiv Soyjaudah, Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications (0975 – 8887), vol. 63, no.16, February 2013.
[13] Y. V. SubhaRao, Abhijit Mitra, S. R. MahadevaPrasanna, "A Partial Image Encryption Method with Pseudo Random Sequences", in: Proceedings of ICISS 2006, LNCS 4332, pp. 315 325, 2006.
[14] Lin Teng, Xingyuan Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive", Optics Communication, 285, pp 4048 – 54, 2012.
[15] Narendra K Pareek, Vinod Patidar, Krishan K Sud, "A Random Bit Generator Using Chaotic Maps", International Journal of Network Security, Vol.10, No.1, PP.32 {38, Jan. 2010.

