MULTI CHAOS-BASED IMAGE ENCRYPTION AND LOSSY COMPRESSION

CHANDRAN. S *

T.RAJESH**

Abstract

The purpose of this paper was to increase the transmission speed and give more secure communication when the image is transmitted through network. In some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, decryption functions will be used to reconstruct the original image. Encryption gives secure communication through network and compression reduce the size of image and increase the transmission speed. The encryption step proposed in this project is chaos based encryption. The two basic properties of chaotic systems are the sensitivity to initial conditions and mixing property. Two chaotic maps, Quadratic and tent maps are used to produce the chaotic sequence and used to control the encryption process. The bitwise XOR operation is used to create encrypted image. After encryption process over, the sender sends encrypted image to network operator. The network operator compressed the image by haar wavelet transform which give high compression ratio, so that storage capacity required will be smaller. In receiver side then decompressed image is decrypted by same symmetric key which is used in sender side. The decrypted image having some noise due to encryption, compression and decryption process, so that noise is removed in decrypted image by image enhancement technique for improve the PSNR value.

***Keywords*—Quadratic Map, Tent Map. Wavelet Compression.**

* P.G.SCHOLAR, DEPARTMENT OF ECE, PSN College of Engineering & Technology, Tirunelveli

** ASSISTANT PROFESSOR, DEPARTMENT OF ECE, PSN College of Engineering & Technology, Tirunelveli

I. INTRODUCTION

The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider may tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. At receiver side, a decoder decryption functions will be used to reconstruct the original image

A. Cryptography

Cryptography is a study of techniques (called cryptosystems) that are used to accomplish the following four goals.

- Confidentiality
- Data integrity.
- Authentication.
- Non-repudiation.

A study of techniques used to break existing cryptosystems is called Cryptanalysis. Since cryptography and cryptanalysis are greatly dependent on each other, people refer to cryptology as a joint study of cryptography and cryptanalysis. Now Let us try to understand all four goals of cryptography. Confidentiality refers to the protection of information from unauthorized access. An undesired communicating party, called adversary must not be able to access the communication material. This goal of cryptography is a basic one that has been always addressed and enforced throughout the history of cryptographic practice. Data integrity ensures that information has not been manipulated in an unauthorized way. If the information is altered, all communicating parties can detect this alteration. Authentication methods are studied in two groups; entity authentication and message authentication. Entity authentication is the process whereby one party is assured of the identity of a second party involved in a protocol, and that the

second has actually participated immediately prior to the time the evidence is acquired. Message authentication is a term used analogously with data origin authentication. It provides data origin authentication with respect to the original message source and data integrity, but no uniqueness and timeliness guarantees. Non-repudiation means that the receiver can prove to everyone that the sender did indeed send the message; i.e., the sender cannot claim that he or she didn't encrypt and/or sign certain digital information.

B. Chaos and Its Use in Cryptography

Chaos theory has been established since 1970s in many different research areas, such as physics, mathematics, engineering, and biology. The most well known characteristics of chaos are the so called "butterfly-effect" (sensitivity to initial conditions), and the pseudo-randomness generated by deterministic equations. (Many fundamental properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. Chaotic systems have several significant features favourable to secure communications, such as ergodicity, sensitivity to initial conditions, control parameters and random like behaviour.

C. The Properties of Chaos

The basic properties of chaotic systems are deterministic, the sensitivity to initial conditions and parameters, the ergodicity and the topological transitivity. Deterministic means that chaotic systems have some determining mathematical equations ruling their behaviour. The sensitivity to initial conditions means that, when a chaotic map is iteratively applied to two initially close points, the iterations quickly diverge, and become uncorrelated in the long term. Sensitivity to parameters causes the properties of the map to change quickly, when slightly perturbing the parameters, on which the map depends. Hence, a chaotic system can be used as a pseudorandom number generator. Topological transitivity is the tendency of the system to quickly scramble up small portions of the state space into an intricate network of filaments. Local, correlated information becomes scattered all over the state space.

D. Image Compression

A digital image, or "bitmap", consists of a grid of dots, or "pixels", with each pixel defined by a numeric value that gives its color. The term data compression refers to the process of reducing

the amount of data required to represent a given quantity of information. Now, a particular piece of information may contain some portion which is not important and can be comfortably removed. All such data is referred as Redundant Data. Data redundancy is a central issue in digital image compression. Image compression research aims at reducing the number of bits needed to represent an image by removing the spatial and spectral redundancies as much as possible.

A common characteristic of most images is that the neighboring pixels are correlated and therefore contain redundant information. The foremost task then is to find less correlated representation of the image. In general, three types of redundancy can be identified as coding redundancy, inter pixel redundancy and psycho visual redundancy.

II. IMAGE ENCRYPTION

Tent and Quadratic chaotic maps are used for image encryption. There are two iterative stages in the chaos-based image cryptosystem. The confusion stage permutes the pixels in the image, without changing its value. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image. To decorrelate the relationship between adjacent pixels, there are n permutation rounds in the confusion stage with $n \geq 1$. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The parameters of the chaotic maps governing the permutation and the diffusion should better be different in different rounds. This is achieved by a round key generator with a seed secret key as input [7].

In the Quadratic map and Tent map, we set initial condition values from the interval(-0.5,0.5).Same value should be used in both sender and receiver side. Encryption process for the proposed system is shown in the following diagram.

The Quadratic map Values are Xored with input image bitwise. After that Tent map values are Xored with the masked image obtained from previous step. Finally we obtained encrypted image with high correlation coefficient value as well as unpredictable histogram image.

ENCRYPTED IMAGE

Fig.1.Image Encryption Process Flow Diagram

A. Quadratic Map

A simple and well-studied example of a map that exhibits complicated behaviour is the Quadratic map from the interval [-0.5,0.5] , parameterized by Xn:

$$X_n = x_n^2 + c$$

Initial condition=-0.5 to +0.5 (1)

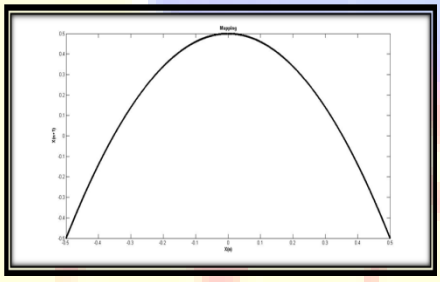

Fig. 2. Quadratic Map

B.Tent Map

In mathematics, the tent map is an iterated function, in the shape of a tent, forming a discrete-time dynamical system. It takes a point x_n on the real line and maps it to another point.

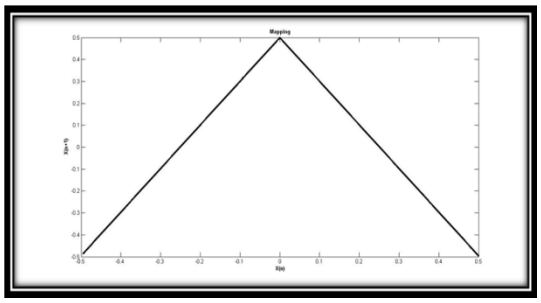

Fig.3. Tent Map

Xn = A - (B (initial condition))

(2)

Initial condition= -0.5 to +0.5

where A and B are positive real constant.

Depending on the value of A, the tent map demonstrates a range of dynamical behaviour ranging from predictable to chaotic.

C. Correlation Coefficient

In order to measure the quantitative similarity between the encrypted image and the original image, the normalized correlation coefficient is used in this project. When both the images are exactly same means the value is 1.When both the images are not exactly same means the value is 0. In this paper for lena image (512*512) I have got the value 0. 0.0198689 which is shown in result section.

$$r = \frac{\sum_m \sum_n \left(A_{mn} - \bar{A}\right)\left(B_{mn} - \bar{B}\right)}{\sqrt{\left(\sum_m \sum_n \left(A_{mn} - \bar{A}\right)^2\right)\left(\sum_m \sum_n \left(B_{mn} - \bar{B}\right)^2\right)}} \quad (3)$$

Where A=Original Image Matrix, and B=Encrypted Image Matrix.

III. HAAR WAVELET TRANSFORM BASED COMPRESSION

The block diagram of Haar Image compression is shown below. The Haar Wavelet Transformation is a simple form of compression involved in averaging and differencing terms,

storing detail coefficients, eliminating redundant data, and reconstructing the matrix such that the resulting matrix is similar to the initial matrix shown below [4].

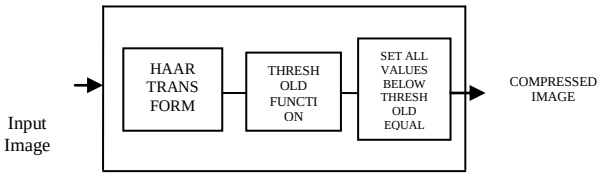

Fig. 4. Block Diagram of Image Compression

The process of averaging and differencing is called Wavelet Transforming matrix. Consider a row in 8*8 matrix [45 11 30 24 45 38 0 23]

Take as pair [45 11],[30 24],[45 38],[0 23].

TABLE 1

RESULT OF AVERAGED AND DIFFERENCED VALUE

Averaged	First Value-Average	Differenced
28	45-28	17
27	30-27	3
41.5	45-41.5	3.5
11.5	0-11.5	-11.5

This new row will have the four averaged values in the first four spaces and the four differences in the last four spaces, respectively.

The value got in the form is [28 27 41.5 11.5 17 3 3.5 11.5]. This technique can't be calculated for large size matrix. For Large size matrix it is calculated as below. Instead of this technique Haar matrix **W** can be used as follows.

1/2	0	0	0	1/2	0	0	0
1/2	0	0	0	-1/2	0	0	0
0	1/2	0	0	0	½	0	0
0	1/2	0	0	0	-1/2	0	0
0	0	1/2	0	0	0	1/2	0
0	0	1/2	0	0	0	-1/2	0
0	0	0	1/2	0	0	0	1/2
0	0	0	1/2	0	0	0	-1/2

Therefore, $W_2 = \begin{bmatrix} \boldsymbol{W_{2*2}} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}$

Similarly, W_3 also calculated like W_2.

Wavelet Transformed Matrix $T = W^T A W$. (4)

Where, W^T = Transpose matrix of W.

A=Original Image.

W=W1*W2*W3.(FOR LEVEL3) (5)

Compressed image matrix C created using the following equation.

Compressed image, $C = (W^T)^{-1} T W^{-1}$ (6)

Where W^{-1} = Inverse of Matrix W.

$(W^T)^{-1}$ = Inverse of Transpose matrix W.

W=W1*W2*W3 (FOR LEVEL3)

T=Wavelet Transformed Matrix

Set a threshold value > 0 and set all of the entries of compressed image matrix with absolute value at most to 0. This matrix now has more 0 values and represents a more compressed image.

IV. IMAGE RECONSTRUCTION

It also follows from this that we can get back to compressed image matrix C using the following equation:

$$\text{Compressed image, } C = (W^T)^{-1} T W^{-1} \qquad (7)$$

Where W^{-1} = Inverse of matrix W.

$(W^T)^{-1}$ = Inverse of Transpose matrix.

V. DECRYPTION

In decryption process set the same initial condition values to the Quadratic map and tent map. Both chaotic mask act as a key in receiver side and original input image is produced by stream cipher operation. Actually decryption is the reverse process of encryption.

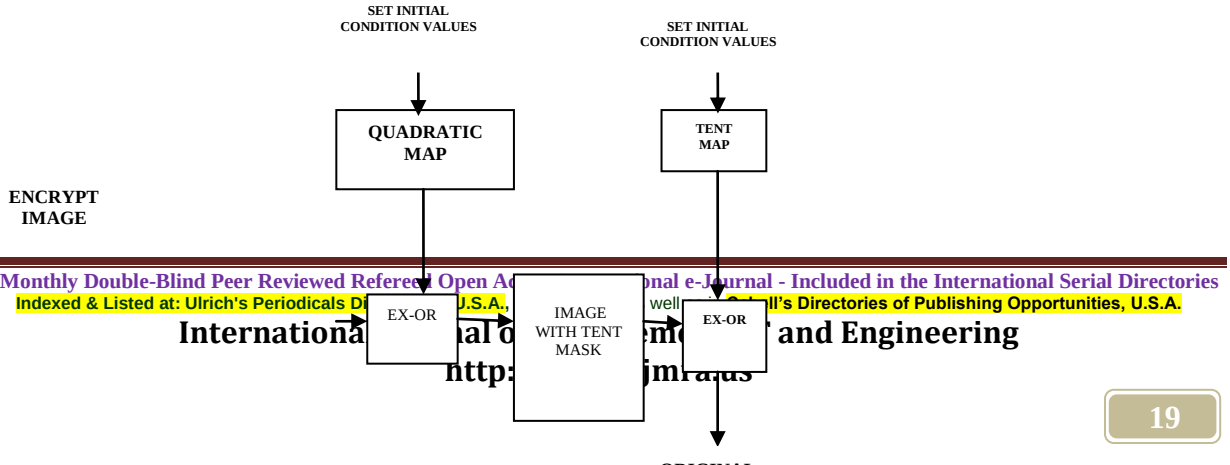

Fig. 3. Image Decryption Process Flow Diagram

VI. RESULTS AND DISCUSSION

The test image Lena sized 512* 512 and baby sized 512*512 shown in Fig. 4,5. was used as the original in the experiment. After encryption of image, attackers can't predict the original image from histogram image. This is shown in fig 4 & fig 5.

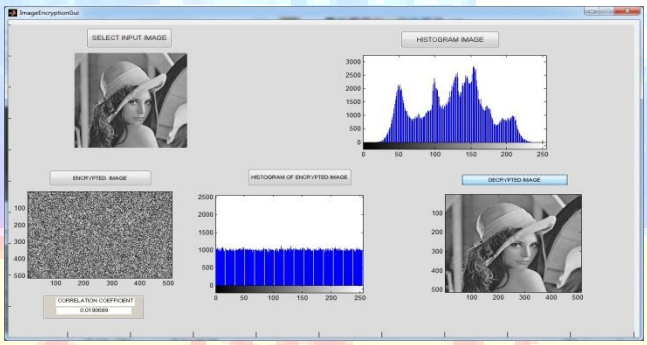

Fig 4.Experiment Result for Lena Image (a) Original image Lena, (b) Histogram of lena image, (c) the encrypted image with correlation coefficient value, (d) Histogram of encrypted lena image, (e)Compressed form of encrypted image, (e)Decrypted Lena Image (f)Reconstructed Image

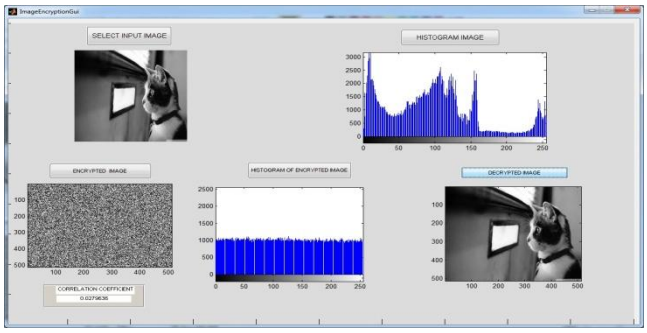

Fig 5.Experiment Result for Baby Image (a) Original Baby Image, (b) Histogram of Baby image, (c) the encrypted image with correlation coefficient value, (d) Histogram of encrypted lena image, (e)Compressed form of encrypted image, (e)Decrypted Lena Image (f)Reconstructed Image

VIII. CONCLUSIONS

The proposed work gives high secure encrypted image using chaos maps. In normal encryption system, from the histogram we can predict the original image easily. But in the proposed system we can't predict the original image from histogram. Haar Compression reduced the memory required to store the images by network operator. Compressed image is decrypted and finally image is enhanced by median filter which gives high PSNR value than the existing system.

REFERENCES

[1] .Gilles Millerioux, José Maria Amigó, and Jamal Daafouz " A Connection Between Chaotic and Conventional Cryptography" in IEEE Transactions on Circuits And Systems—I: Regular Papers, VOL. 55, NO. 6.,pp.1695- 1703, JULY 2008.

[2].Mark Johnson, Student Member, IEEE, Prakash Ishwar, Vinod Prabhakaran,Student Member, IEEE," On Compressing Encrypted Data"in IEEE Transactions on Signal Processing, VOL. 52, NO. 10,pt. 2, pp. 2992–3006, October 2004.

[3]. Rohit Arora, Madan Lal Sharma, Nidhika Birla," An Algorithm for Image Compression Using 2D Wavelet Transform" in International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 4.,pp. 2758- 2764, Apr 2011.

[4]. Samson.Ch., Sastry.V.U.K. "A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform" in International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 9, ,pp. 178-183, 2012.

[5].Sathishkumar.G.A. Dr.Bhoopathy.K bagan and Dr.Sriraam.N "Image Encryption Based On Diffusion And Multiple Chaotic Maps" in International Journal of Network Security & Its Applications (IJNSA), March 2011,Vol.3, No.2. pp. 181-194, March 2011

[6]. Wei Liu, Member, IEEE, Wenjun Zeng, Senior Member, IEEE, Lina Dong, andQiuming Yao "Efficient Compression of Encrypted Grayscale Images" in IEEE Transactions on Image Processing, VOL. 19, NO. 4, pp. 1097-110,2APRIL 2010.

[7].Xinpeng Zhang "Lossy Compression and Iterative Reconstruction for Encrypted Image" in IEEE Transactions on Information Forensics and Network Security, VOL. 6, NO. 1,pp. 53-58.,March 2011.