A NOVEL METHOD OF IMAGE ENCRYPTION USING LOGISTIC MAPPING

Nidhi Sethi[1]
Asstt. Prof.
Dehradun Institute of Technology, Dehradun-248001
Uttrakhand , India
nidhipankaj.sethi102@gmail.com

Deepika Sharma[2]
Lecturer
Dehradun Institute of Technology, Dehradun-248001 Uttrakhand , India
deepika4mjaspur@gmail.com

Abstract—**In this paper, we proposed a new method to develop secure image-encryption techniques using a logistics -based encryption algorithm. In this technique, a Haar wavelet transform was used to decompose the image and decorrelate its pixels into averaging and differencing components. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion properties. The remaining components (the differencing components) are compressed using a wavelet transform. Many test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission. To send the keys in secure form steganography will be used. Steganographic techniques allow one party to communicate information to another party without a third party even knowing that the communication is occurring**

Keywords- **Image encryption, Haar wavelet, logistics mapping, Steganography**

Introduction

In last few decades, digital information sharing has become more common with the fast development of Internet. However, in open networks, it is very much important to keep sensitive information such as military and medical images secure from becoming vulnerable to unauthorized access. The development of fast and efficient cryptographic and steganographic schemes is thus essential to the provision of multimedia security. Paper[5] states that ,with the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Pixels are the basic elements of an image, so in order to encrypt an image we have to encrypt the information hidden in each pixel. Pixel's position values can also be used for encryption purpose. Technique of image encryption should be strong enough so that the encrypted image could contain good properties that may undergo most of the testing criteria. In our work we encrypt the image using logistic mapping along with transformation, transformation is a process of encoding data to another form by removing all the redundancy that occurs in the data. This encoding technique will change the data into unreadable form as well as extracting the low-low band of the data file. Haar Wavelet is used in our method for transformation of the image which is further fed to encryption algorithm for confusion and diffusion. For solving the problem of transmission of keys we have watermarked the keys in encrypted image.

A. Litreature Review

Information security is the hot topic of research for decades to deal the prevailing security requirements. Traditional encryption schemes such as DES,T-DES, AES are not suited to build the cryptosystem for digital images , this is due to the inherent features of the images and high redundancy. J. M. Blackedge et al. [2] have proposed a multilevel blocks scrambling is employed to scramble the blocks of coefficients which requires high computation. The control parameters of the scrambling are randomly generated from the secret key dependent. The key stream used to encrypt the scrambled image is extracted from the chaotic map and plain image.

W Puech et al. [13] have explained and reviewed the security, performance and reliability issues , in respect to the combination of various chaos based symmetric key cryptosystems. Logistic , Henon , Tent , Cubic and Cheyshev mappings have been used for the enhancement of the key space. Cheng qing Li et al. [13] , have reviewed four chaos based image encryption schemes were proposed .Essentially, the four schemes can be classified as one class , which composed of two basic parts :permutation and diffusion of pixel value with cipher text feedback function. Hence following security problems were found: 1) the schemes are not sensitive to change of plain-image; 2) the schemes are not sensitive to change of secret key; 3) there exist a serious flaws of diffusion function; 4) the schemes can be broken with no more than [$\log_l$(MN)+3] chosen images when iteration number is equal to one, where MN is dimension of image.

S. K. Muttoo et al. [15] has proposed Data Hiding in JPEG images, which has been **o**ne of the well known embedding method of stenography based on Transform domain is JPEG-JSTEG which embeds secret message (that is, in encoded form with help of Huffman codes) into LSB of the quantized DCT coefficients. Microslav Dobsicek et al. [16] in his article "Modern Stenography" has stated that there are almost few bytes ,one can play with, without destroying carried information.LSB is well known method. A color of pixel is coded in 3 bytes array of indices to RGB palette. If we change only LSB bit in each color element, then the picture will seem still the same.

B. Proposed Algorithm

The proposed image encryption algorithm has two major steps: Transformation and Encryption. Firstly, the transformation has been done using Haar Wavelet transform. The haar function is :

$$\psi(t) = \begin{cases} 1 & t \in [0, 1/2) \\ -1 & t \in [1/2, 1) \\ 0 & t \notin [0, 1) \end{cases}$$

And

$$\psi_i^j(t) = \sqrt{2^j}\psi(2^j t - i),\ j = 0, 1, \ldots \text{ and } i = 0, 1, \ldots, 2^j - 1 \text{ .}$$

Haar Transform is only about averaging and differencing. By applying the Haar wavelet transform we can represent the image in terms of a low-resolution image and a set of detail coefficients The detail coefficients are used in reconstruction of the image. The low-low band is fed to second phase. Secondly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. To achieve this, a block based image shuffling scheme is proposed using crossover techniques of genetic algorithm. Then the pixel values of the shuffled image are encrypted by applying a 1 D Logistic map. The control parameters of crossover techniques are the control parameters of shuffling. The shuffling effect obtained after a number of iterations , depends upon the parameters and the number of iterations . In this algorithm, the control parameters are chosen by the users which are served to 1 D Logistic mapping.

The secret keys are sent by watermarking method to the receiver end. The embedding key is sent by some secure channel. This technique aims at enhancing the security level of the encrypted images and the secret keys by hiding the keys in the encrypted image itself. The Fig 1. explains the whole process .

Extraction, Decompression and Decryption **:** Using the above algorithm in reverse order ,we can find the original keys and the original image.

C. Analysis:

Key Analysis :

i) Key Space: Key space is the total number of different keys that can be used in the cryptographic system. A cryptographic system should be sensitive to all secret keys. There are total three initial conditions of chaotic map used in the algorithm and the initial conditions of logistic maps used as secret keys of encryption and decryption. In our case, the precision is 10^{-14}, the key space size is $(10^{14)8}$ $=10^{112}$ **.**This keyspace is large enough to resist brute force attack

ii) Key Sensitivity: Our proposed encryption algorithm is sensitive to a small change in the secret keys. If we change a little $(10^{-14)}$ any of the initial conditions then the decrypted image is totally different from the plain-image.

Differential analysis**:**

In image encryption, the resistance to differential attacks by the cipher image is commonly measured by the NPCR and UACI tests . The NPCR(Number Pixel Change Rate) and UACI(Unified Average Change Intensity) , MAE(Mean absolute Error) are used to test the number of changing pixels and the number of averaged changed intensity between ciphertext images, respectively, when the difference between plaintext images is subtle (usually a single pixel).The following results have been tested for following images by performing 4 rounds of encryption. For results refer Table 1.

Information Entropy :

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [14]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy *H*(*m*) of a message source *m* can be calculated as:

$$H(m) = \sum_{i=0}^{2N-1} P(m_i)\log_2 \frac{1}{P(m_i)},$$

For results refer Table 2.More is the entropy better is the encryption.

PSNR AND MSE

The PSNR(peak signal to noise ratio) is most commonly used as a measure of quality of the image. It is an engineering term, the ratio between the maximum power of a signal and the power of corrupting noise.

PSNR= 10 log10 (Max signal^2/MSE)

MSE (mean square error) measures the average of the squares of the errors. The MSE is the cumulative squared error between the encrypted and the original image,

Experimental Results

The proposed algorithm is implemented in MATLAB 7.0 . The total number of keys are 4 . Key 1: Fed to random number generator for further processing , Key 2: Number of iterations ,Key 3: 0.3915; (initial parameter for logistic mapping) Key 4: 3.9985;(3<key3<4).The results has been analysed by the above stated methods . Fig 2: shows the results. Fig: 3 Shows the histogram of the original and encrypted images.

D. Conclusions:

The reported paper aimed at developing an algorithm for using wavelet techniques along with the encryption based on the concept of shuffling the pixels positions and changing the gray values of the image pixels. To perform the shuffling of the plain-image's pixels, a block based shuffling scheme is proposed, in which the plain-image is decomposed into 8x8 size blocks and a cross-over mutation operation of genetic algorithm, is applied in three different ways to achieve good shuffling effect. Moreover, the control parameters of shuffling are randomly generated using a 2D coupled Logistic map to enforce the secrecy of the image.We concluded that the encryption algorithm has shown good results in terms of PSNR, MSE,NPCR and , UACI.

E. Figures and Tables

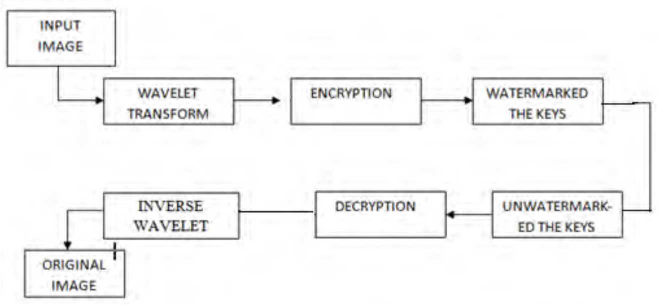

Fig1: Block Digram of the proposed algorithm

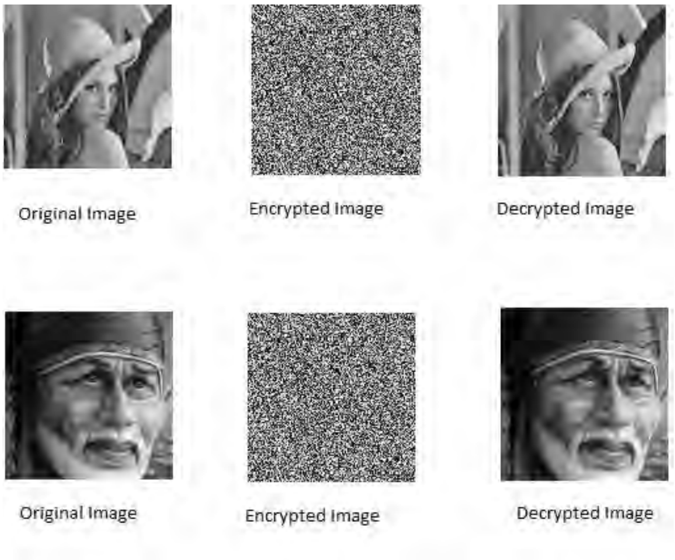

Fig:2 Results

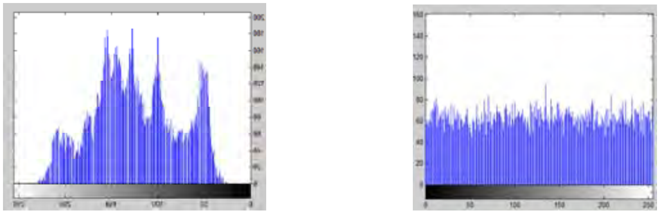

Fig3: Histogram a)original image(lena)b) encrypted image(lena)

TABLE 1 (NPCR , UACI and MAE)

S N	Name of the image	Size	NPCR	UACI	MAE
1	Baba.jpg	128*128	0.00610	0.002656	59.08
2	Lena.bmp	128*128	0.00610	0.002010	53.67
3	Brain.jpg	256*256	0.00152	0.009155	79.46
4	HR.png	240*240	0.00173	0.000456	47.59

TABLE 2: Information Entropy

S. N	Name of the image	Size	Plain image	Cipher image
1	Baba.jpg	128*128	7.7153	7.5830
2	Lena.bmp	128*128	7.9894	7.9891
3	Brain.jpg	256*256	5.3581	7.9974
4	HR.png	240*240	6.52124	7.9956

TABLE 3:PSNR and MSE

S. N	Name of the Image	No. of keys	MSE	PSNR
1	Lena.bmp	03	0.0070	69.7082
2	Baba.jpg	03	0.0051	71.0960

a)Hist. of Original Image(lena.bmp) b) Hist of encrypted image

References

[1] P Raviraj and M.Y. Sanavullah, “The modified 2D-Haar Wavelet Transformation in image compression” Middle East Journal of Scientific Research, Vol: 2 , Issue: 2,pp 73-78,ISSN 1990-9233, Apr-Jun, 2007.

[2] Jonathan M.Blackedge,Musheer Ahmed ,Omar Farooq “Chaiotic image encryption algorithm based on frequency domain scrambling” ,School of Electrical Engineering systems Articles,Dublin Institute of Technology ,2010.

[3] G. K. Kharate, A. A. Ghatol and P.P.Rege,”Image Compression Using Wavelet Packet Tree”, ICGST-GVIP Journal, Volume Issue (7), July 2005.

[4] David F. Walnut, “Wavelet Analysis”, Birkhauser,2002, ISBN-0- 8176-3962-4.

[5] Musheer Ahmed, M.shamsher Alam **“**A new algorithm of encryption and decryption of images using chaotic mapping**”** International Journal on computer science and engineering,vol.2(1), 2009,pp46-50.

[6] Mazleena Salleh1, Subariah Ibrahim2 & Ismail Fauzi Isnin3“Image encryption algorithm based on chaotic mapping” IEEE conference on circuits and system,vol.2,2003.508-511.

[7] J.Fridrich **“S**ymmetric ciphers based on two-dimensional chaotic maps” International Journal of Bifurcation and Chaos.vol.8, 1998,1259-1284.

[8] **L**inhua Zhang, Xiaofeng liao , Xuebing Wang “An image encryption approach based on chaotic maps” chaos solitons and fractals,vol.24 2005,759-765.

[9] **S**higuo lian , Jinsheng sun, Zhiquan wang **“**A block cipher based on a suitable use of the chaotic standard map” chaos solitons and fractals,vol.26, 2005,117-129.

[10] Ahmed T A1-Taani and Abdullah M.AL-Issa”A Novel Steganographic Method For Gray-Level Images”, World Academy Of Science, Engineering and Technology,2009.

[11] Alkhraisat Habes “Information Hiding in BMP image Implementation, Analysis and Evaluation” Saint Petersburg Institute for Informatics and Automation, Russian Academy of Sciences, Saint Petersburg, Russia Received February 26, 2006

[12] Puech, W. and Rodrigues, J. M. A New Crypto- Watermarking Method for Medical Images Safe Transfer. In The 12th European Signal Processing Conference, pp. 1481-1484, Sept. 2004.

[13] Chengqing Li, “On the security of a class of Image Encryption Scheme”, IEEE International Symposium on Circuit & System ,2008 ISCAS, Department of Electronics Engineering, University of Hong Kong , pg 3290-3293

[14] S. K. Muttoo1, Sushil Kumar **“**Data Hiding in JPEG Images**”** BVICAM’S International Journal of Information Technology Bharati Vidyapeeth’s Institute of Computer Applications and Management, New Delhi.

[15] Microslav Dobsicek, “Modern Stegnography” 8th International Student Conference on Electrical Engineering FEE CTU 2004.