Hash Based Four Level Image Cryptography

Jagminder Kaur Cheema, Mandeep Singh Sandhu, Sukhveer Singh
[1, 2] *Computer Science Engineering, BMSCE Muktsar*
Punjab India
[1]*cheemajimmi@yahoo.co.in*
2 write_mandeep@yahoo.co.in
[3]*Electronics and communication Engineering, BMSCE Muktsar*
Punjab India
[3]*sukhveer29@gmail.com*

***Abstract*— the paper presents a four level image encryption cryptography based on hash i.e. a replacing table for giving new values to the pixels. The basic motive of this work is to provide a technique for securing the images to the level that one is not able to recognize it while transmission to prevent the attack of intruders. In this paper multi level image cryptography is used based on chaotic system which employs random integer function for the diffusion phase. The proposed algorithm provides large key space. Results are compared in terms of correlation coefficient which satisfies the property of zero correlation. In this paper it is proposed that multi level image cryptography to securely encrypt the images for the purpose of storing images and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that it makes the encrypted image with a constant increasing intensity. The second advantage is that it does not impose any restriction on the decoding of the specific image signal because with every new image signal it produces a new hash accordingly. Our system would be systematically evaluated, and it shows a high level of security with excellent image quality**.

***Keywords*-Replacing, Correlation, Random Integer, Chaotic, Cryptography**

*****

I. INTRODUCTION

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. It is argued that the encryption algorithms, which have been originally developed for text data, are not suitable for securing many real-time multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and video data in commercial systems. Hardware implementations, on the other hand, add more cost to service providers and consumer electronics device manufacturers. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "*selective encryption*" where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bit stream to obtain a fast method [2]. With the rapid progress of Internet, in recent years, to establish the transmission of images, highly reliable and high-speed digital transmission is required. Besides this, Internet applications have to deal with security issues. Internet users exasperate potential security threats such as eavesdropping and illegal access. They want to be protected and to ensure their privacy. Network security and image encryption has become important and high profile issues. Most traditional or modern cryptosystems have been designed to protect textual data. An original important and confidential plaintext is converted into cipher text that is apparently random nonsense. Once the cipher text has been produced, it is saved in storage or transmitted over the network. Upon reception, the cipher text can be transformed back into the original plaintext by using a decryption algorithm. However, images are different from text. Although we may use the traditional cryptosystems (such as RSA and DES-like cryptosystems) to encrypt images directly, it is not a good idea for two reasons. One is that the image size is much greater than that of text, so the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image; a

decrypted image containing small distortion is acceptable due to human perception.

II. ENCRYPTION PROCESS

In this thesis we use multi level cryptography. Cryptography is the art and science of writing in secret codes. A general cryptographic system includes two processes further in it to work:

1. Encryption
2. Decryption

In encryption we encrypt the image to make it to unreadable form for secure transmission and information hiding and in Decryption we restore back the image to its original form. A number of techniques are available for encryption, what we are using is multi level encryption and decryption. By shifting rows and columns of pixels we scramble the image and then diffusion is used i.e. we use chaos based method. In a general chaos based system there are two stages of complete encryption process:

1. Confusion
2. Diffusion

In the confusion phase, a 2-D or a higher dimensional chaotic map is employed to relocate almost all pixels in the image or the information of the different pixels is mixed. In the diffusion phase, all the pixels are treated as 1-D array, where the values of the pixels are modified sequentially. In this thesis we employ four levels of encryption. In the first level the rows of pixels are shifted column wise and in second level columns of pixels are shifted row wise that is scrambling is done in the first two levels. Then in third phase pixels are arranged in 1-D array and arranged according to the increasing intensity values of pixels to generate a key Then random Integer function is used to generate random values for each pixel intensity to change the whole image .Then in decryption the keys generated in level third and fourth are used to restore back the image and then columns of pixels and then rows of pixels are shifted to restore the image to its original form. [21]

III.STEPS OF ENCRYPTION ALGORITHM

Step 1.Read the color image I_{m*n}, where m and n is the height and width of image respectively

Step 2.Scramble the image by shifting half of the rows column wise by a step of two at first level of encryption.

Step 3.scramble the image by shifting half of the columns, row wise by a step of two at second level of encryption.

Step 4.Convert the image to one dimensional array sort the pixels in increasing order of intensity at third level of encryption.

Step 5.Replace pixel's intensity value by adding one to the values generated by the random integer function at fourth level of encryption.

Decryption process is the inverse of encryption process.

IV.EXPERIMENTAL RESULTS AND STATISTICAL ANALYSIS

A. Simulation results

In this paper experimental analysis of the proposed algorithm has been done with a color flower and butterfly image and MATLAB 7 is used to realize the algorithm. Simulation results are shown as Figure

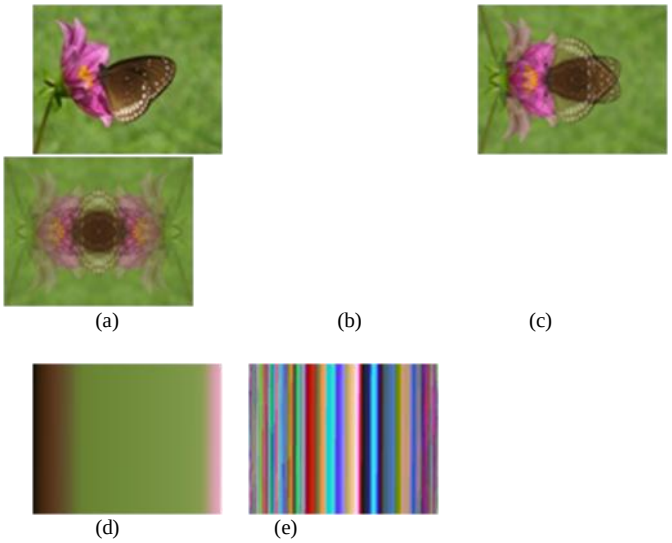

Figure 1.Encryption images: (a) Original image (b) Scrambled image at level 1 (c)Scrambled image at level 2 (d)Scrambled image at level 3(e) Multi level encrypted image

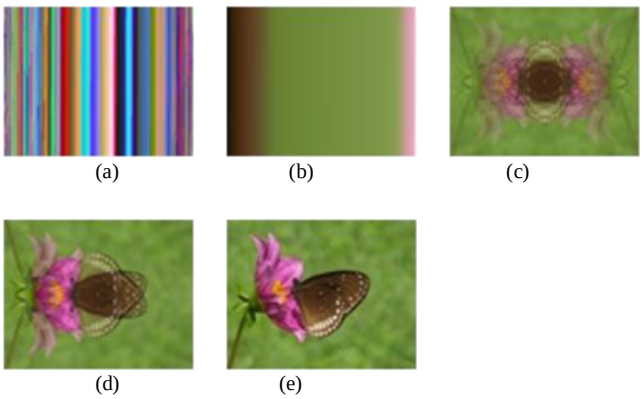

Figure 2.Decryption images: (a)Encrypted image (b)Decrypted image at level 2 (c)Decrypted image at level 3 (d)Decrypted image at level 4 (e) Original image

B.Statistical analysis

(a)Histogram analysis

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. . The histogram of the cipher image as shown in fig 3, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is significantly different from the respective histograms of the original image and hence does not provide

any clue to employ any statistical attack on the proposed image encryption procedure. [12][6]

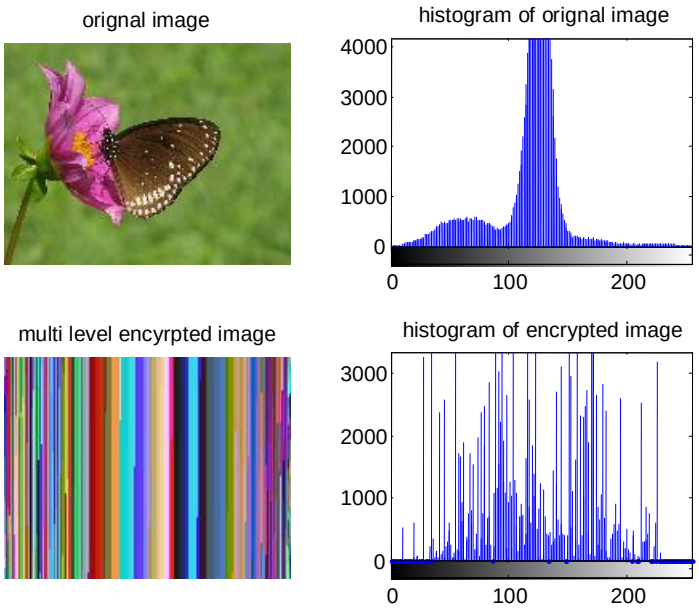

Fig 3:Histograms of plain and ciphered image.

(b)Correlation analysis

To test the correlation between two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels respectively in encrypted image, Firstly randomly select n pairs of two adjacent pixels from an image and then calculate correlation coefficient r_{xy} using these equations

$$r_{xy}= \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

Where x and y are grey scale values of two adjacent pixels in the image.In numerical computations following formulas is used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

$$Con(x,y)= \frac{1}{N}\sum (x_i - E(x))(y_i - E(y))$$

The Table I lists the correlation coefficients of the encrypted images in horizontal,vertical and diagonal axis showing no detectable correlation exist between the original image and its corresponding encrypted image.

Table I: CORRELATION COEEFICIENTS OF TWO ADJACENT PIXELS IN THE ORIGINAL AND ENCRYPTED IMAGES BY PROPOSED METHOD

AXIS	ORIGINAL IMAGE	ENCRYPTED IMAGE
CORR.HORIZONTAL	0.1337	-0.012023
CORR.VERTICAL	0.11764	0.03364
CORR.DIAGONAL	0.1453	-0.24406

III. CONCLUSION

In this paper it is proposed that multi level image cryptography to securely encrypt the images for the purpose of storing images and transmitting them over the Internet. There are two major advantages associated with this system. The first advantage is that it makes the encrypted image with a constant increasing intensity. The second advantage is that it does not impose any restriction on the decoding of the specific image signal because with every new image signal it produces a new hash accordingly. Our system would be systematically evaluated, and it shows a high level of security with excellent image quality.

REFERENCES

[1] Fei Xiang Xiao Guo -FeicongXiang Xiao-cong Guo "An Image Encryption Algorithm based on Scrambling and Substitution usingHybrid Chaotic Systems" 2011 IEEE
[2] Mythili Paul A.J, P., Jacob K. Paulose "Matrix based Cryptographic Procedure for Efficient Image Encryption" 2011 IEEE.
[3] Wang Ran-Zan and Hsu Shuo-Fang "Tagged Visual Cryptography" NOVEMBER 2011 IEEE.
[4] Dutta Agniswar , Sen Abhirup Kumar, Das Sankar, Agarwal Shalabh and Nath Asoke "New Data Hiding Algorithm in MATLAB using Encrypted secret message" 2011 Crown Copyright.
[5] Xiaolin Xu and Jiali Feng "Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector" 2010 IEEE.
[6] Kamali Seyed Hossein, Shakerian Reza, Hedayati Maysam and Rahmani Mohsen "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 IEEE.
[7] Panda Jeebananda and Bisht Jagat "Digital Image Watermarking In Integer Wavelet Domain Using Hybrid Technique" 2010 IEEE.
[8] Jing Fan, Honglian Li "A New Image Content Protection Method" 2010 IEEE
[9] Kuang Li-Qun, Zhang Yuan, Han Xie "A medical image authentication system based on reversible digital watermarking" 2009 IEEE.
[10] Nien H. H., Huang W. T., Hung C. Chen M. S. C., . Wu S. Y, Huang C. K. and Hsu Y. H. "Hybrid Image Encryption Using Multi-Chaos-System" 2009 IEEE.
[11] . Kumar Anil and Makur Anamitra "Lossy Compression of Encrypted Image by Compressive Sensing Technique" 2009 IEEE.
[12] Yu Hai, Zhu Zhiliang and Chen Guanrong "An Efficient Encryption Algorithm Based on Image Reconstruction" 2009 IEEE.
[13] Yun-peng ZHANG , Zheng-jun ZHAI, Wei LIU and Xuan NIE "Digital Image Encryption Algorithm Based on Chaos and Improved DES" October 2009 IEEE

[14] . Nisar A. Memon, S.A.M. Gilani, and Asad Ali "Watermarking of Chest CT Scan Medical Images for Content Authentication" 2009 IEEE.

[15] Chang Kuo-Huang,Chen Yi-Cheng ,Hsieh Chung-Cheng,Huang Chi-Wu andChang Jeng Chi "Embedded a Low Area 32-bit AES for Image Encryption/Decryption Application" 2009 IEEE.

[16] . Liu F,Wu C.K. ,Lin X.J "Colour visual cryptography schemes"July 2008 IET Information Security.

[17] Hamdi Mohamed and Boudriga Noureddine "Chaotic Progressive Access Control for JPEG2000 Images Repositories" 2008 IEEE.

[18] Rhee Keun-Moo "Image Encryption Using Self Regressive Function" 2008 IEEE

[19] Ito Masanori ,Ohnishi Noboru,Alfalou Ayman ISEN-Brest andMansour Ali ENSIETA "New Image Encryption and Compression Method Based on Independent Component Analysis" 2008 IEEE.

[20] Our Yang,Lee Won-Young andRhee Kyung Hyune "A flexible JPEG2000 image encryption based on arithmetic coding" 2007 IEEE

[21] Ravishankar K. C., Venkateshmurthy M.G." Region Based Selective Image Encryption" 2006 IEEE.

[22] YU F. Q,ZHANG Z. K,XU M. H "A digital watermarking algorithm for image based on fractional Fourier transform" 2006 IEEE.

[23] Lin Qiu-Hua ,Yin Fu-Liang, andZheng Yong-Rui" Secure image communication using blind source separation" 2004 IEEE.

[24] SchyndeP R.G. van ,Tiekel A.Z. ,Svalbe I. D "Key independent watermark detection" 1999 IEEE.