ISSN 2278-3091

Volume 3, No.5, September - October 2014

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://warse.org/pdfs/2014/ijatcse01352014.pdf

IMAGE ENCRYPTION USING A COMBINANTION OF HAAR AND DNA ALGORITHM

[1]Rohit Kumar, [2] Bhanu Pratap, [3] Vaibhav Singh

[1]M. Tech Scholar, Department of Comp.Sci.and Engg., Graphic Era University, Dehradun
[2] M. Tech Scholars, Department of Comp.Sci.and Engg., RCE, Roorkee
[3] M. Tech Scholars, Department of Comp.Sci.and Engg., DBIT, Dehradun

[1]kambojrohit42@gmail.com
[2]vai.rajput123@gmail.com
[3]bhanu8909@gmail.com

***Abstract*— 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 schemes is thus essential to the provision of multimedia security. Information security becomes more important with the fast progression of data exchange in electronic form. 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 first compress the image using Haar wavelet transformation and then encrypt it using DNA algorithm. Wavelets are mathematical functions that were developed for sorting the data by frequencies. A Wavelet transformation converts data from the spatial into the frequency domain and then stores each component with a corresponding matching resolution scale. By applying the Haar wavelet transform we can represent this image in terms of a low-resolution image and a set of detail coefficients. Haar Transform is nothing but averaging and differencing. DNA algorithm is used for further encrypting the image. This technique will change the data into unreadable form.**

***Keywords*— DNA, Cryptography, Compression, Wavelet, Encryption**

1.INTRODUCTION

Nowadays Digital Images find a lot of applications almost in all the fields, for e.g. Information Hiding, Communication etc. Security of these images is very important. Image encryption is one method of providing security to digital images.

Encryption is a method of converting original data or information, called clear text or plaintext, into a form that is unreadable by any unauthorized person that is called cipher text. Plaintext can be read by a computer or any person without any secretes information. When it is converted into the cipher text, no one (human beings and any computer machines) is able to process it until it is converted into readable form from decrypted form. This enables s to send any type of information or data over any network without any security breach. When any data or information is stored on a storage media, it is protected by physical and logical access controls. When we need to sand this stored data or information over any insecure channel or network, network does not take any guaranty of these controls.

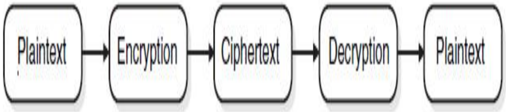

Fig: 1.1 The process of encryption and decryption.

A cryptosystem is created through hardware components or application program code, which provides encryption and decryption of data and information. The cryptosystem makes use of mathematical algorithm for encryption process, which determines the complexity of the encryption and decryption process. This mathematical algorithm is applied over plain text in specific sequence to convert it into unreadable form. Most encryption algorithms makes use of a key, which is required to encrypt and decrypt the given data or information, as shown in below Figure.

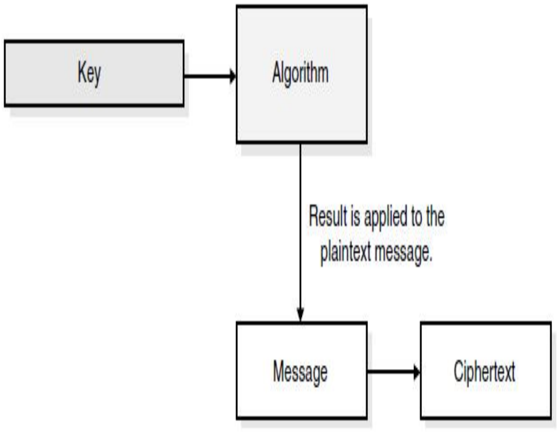

Fig: 1.2 The key is inserted into the mathematical algorithm and the result is applied to the message, which ends up in cipher text.

The algorithm, the set of mathematical rules, dictates how enciphering and deciphering take place. Some algorithms are public and security of these algorithms are total dependent on secrete key. We can hide the encryption algorithms used for encryption and decryption process from public, but most of the algorithms are publicly known and well understood. If mechanisms of the algorithm used for encryption and decryption is already known, then something must be secrete. That secrete part of encryption algorithm is the key used for encryption and decryption process. The key is made of random bits and it can be any value. Each algorithm makes use of key space. The key is constructed using random values within the key space of algorithm. The larger the key space, larger the values of keys we can used to show differ keys.

2. RELATED WORK

Over the years many different methodologies have been introduced for image encryption for secure transmit ion of images over networks .Previous encryption schemes such as, AES DES and T-DES are not well suited to make the cryptosystem for digital images, the main cause of this the inherent features of the images and high redundancy. Some related work is explained below:

A) Image Encryption Using Block-Based Transformation Algorithm: Encryption is the process by [1] which data is securely transmit in unsecured networks (i.e. internet). Every kind of data has itself values; So many unique security services or techniques should be used to guard secret image data from malicious access. Today's many of the encryption algorithms are use for textual data and they may not be fine for multimedia data such as images or pictures. We used a Blowfish algorithm which is based on the combination of image transformation and encryption, decryption algorithm. The Real image is divided into several blocks, with the help of transformation algorithm the image were rearranged into a transformed image.

B) An [2] RGB Image Encryption with the help of Wavelet-based Compression: we have prepared a new methodology for an RGB image encryption. Which is supported by lifting scheme base on lossless compression? First of all we take the color image as an input & then we have compressed this input color image by using a Two -Dimensional integer wavelet transformation method. Then in next step we have applied the lossless predictive coding method to get additional compression. After the compression a compressed image is encrypted with the help of Secure Advanced Hill Cipher .which involving , an operation called XOR and a function called Mix (). Decryption followed by reconstruction & the decryption process shows that there is no any difference between the output color image and the input color image. This proposed method can be used for secure transmission of image data.

C) Image Compression Using Haar Wavelet Transform: Compression is a technique by which a raw binary coded data is reduced from its original size i.e. raw binary coded data got some changes after compression. But compressing an image is different than compressing raw binary data. Some compression methods can be used to compress images but with the optimal result. The reason of this is because images have some statistical attributes and some of the details in the image can be exploited by encoders and for saving a little more bandwidth or storage area. This also means that in this area the lossy compression techniques can be used. We have [3] implemented HAAR Wavelet Transform. The discrete wavelet is mainly sub band–coding system & the sub band coders have been fully successful in speech and image compression. PSNR (Peak Signal Noise Ratio) and MSE (Mean Square Error) proves that the image compression done by HAAR transformation. And The Quantization process is complete by dividing the image matrix into some different blocks and taking mean of the pixel in the given particular block. So it is clear that Discrete Wavelet Transformation (DWT) has very useful application in the compression related problems. And other hand the use of Haar transform is well suited.

D) Image Encryption with the help of Compression Using Multilevel Wavelet Transform: we introduce a better approach for image encryption. Input image is decomposed with the help of [4] multilevel 2-D wavelet transform, and threshold is applied on the decomposed structure to get compressed image. The next step is encryption by decomposing the compressed image with the help of multi-level 2-D Haar Wavelet Transform (maximum allowed decomposition level). The results are in the corresponding bookkeeping matrix S and the decomposition vector C. The reshaped vector is rearranged by performing permutation to produce encrypted image. After that the decomposition vector C is reshaped into the size of the input image.

E) Image encryption method using logistic mapping: we introduced a advance method to develop secure image-encryption techniques with the help of [5] logistics -based encryption algorithm. For decompose the image and decor relates its pixels into some differencing components, we used a Haar wavelet transform. The logistic based encryption algorithm produces a cipher of the test image that has good diffusion and confusion attributes.

F) Comparing image encryption methods using new transformation technique: Randomness can be easily created using chaotic sequences. a new encryption scheme based on two phases has been introduced. Firstly image Is converted using a new transformation technique and then image pixels are shuffled using [6] Chirikov Standard map. Image pixels are shuffle at random using modified logistic map. Image encryption based on this approach does not provide any relation between plain and encrypted image. Security of this method depends upon key

G) Image segmentation based on wavelet transformation: [7] Many applications of multi-dimensional signal processing makes use of image segmentation. Wavelet transformation can be used for feature extraction of image pixels and also compared them with watershed transformation. Haar wavelet transformation is a efficient method for extracting feature of image pixels. The algorithm provides good results and efficiently used for any image.

H) A Novel Image Encryption Algorithm [8] Based on DNA Subsequence Operation: Based on DNA subsequence a better cryptosystem has been proposed.
Here only DNA sub sequence operation is used hence it does not have any match with traditional DNA approach for encryption. Location and the value of pixel of image is scramble using logistic chaotic map. Encryption process based on this approach has good security and efficiency.

3. IMAGE ENCRYPTION USING HAAR WAVELET AND DNA ALGORITHM

In this section we will present the scheme used for image compression and image encryption along with the algorithm of Haar wavelet transformation and DNA technique. The basic idea behind the thesis is to first compress the image so that we can sand it over the network quickly and encrypt it so that we can transmit it over any network securely and safely.

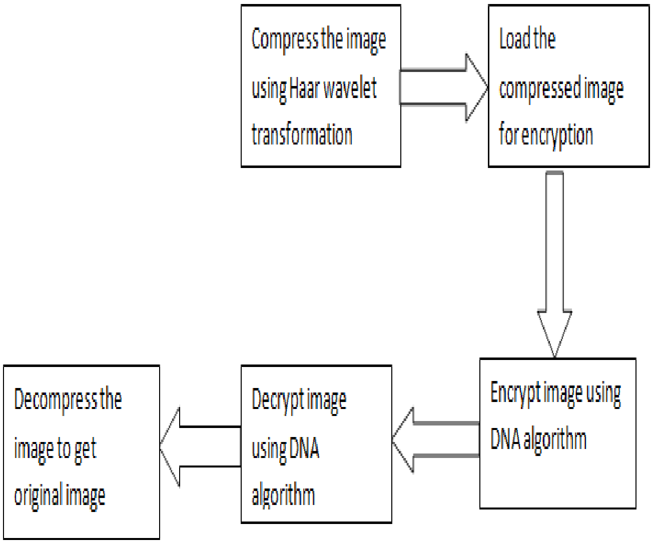
Compress the image using Haar wavelet transformation
Load the compressed image for encryption
Encrypt image using DNA algorithm
Decrypt image using DNA algorithm
Decompress the image to get original image

Fig: 3.1.1 Image encryption and decryption process

For compressing the image we have designed a GUI in Matlab. The GUI processes the image in matrix form, we first compress the image by dividing the image matrix into blocks and taking mean of the pixel in the given blocks using [11]Haar based algorithm and then apply DNA algorithm for encrypting the image. After encrypting the image we can securely transfer the image over any network.

The first DWT [21] was invented by the Hungarian mathematician Alfred Haar. For an input represented by a list of numbers, the Haar wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale, finally resulting in differences and one final sum.

- First we compress the image using Haar wavelet transformation.
- Wavelets are a set of mathematical bases function.
- When approximating a function in terms of wavelets, the wavelet basis functions are

selected according to the function being approximated.

- Wavelets employ a dynamic set of basis functions that represents the input function in the most efficient way.
- Thus wavelets are able to provide a great deal of compression and are therefore very popular in the fields of image and signal processing.

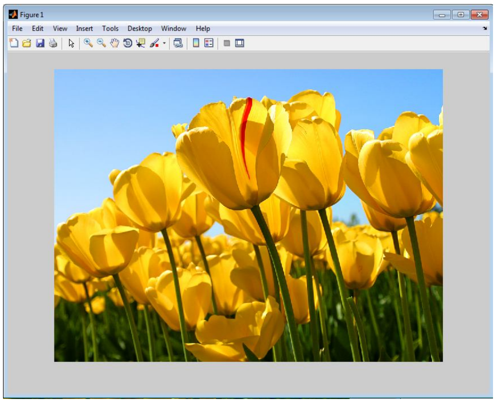

Fig:3.1.2 Original Image

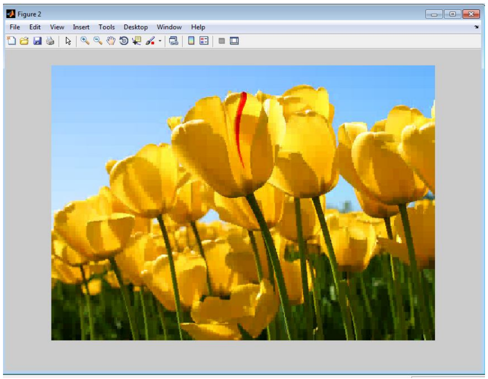

Fig:3.1.3 Compressed image

3.2 IMAGE ENCRYPTION USING DNA ALGORITHM

- DNA encryption means combining DNA technique with cryptology and producing new cryptography to provide safe and efficient cipher services.

- Here we propose a method of image encryption based on DNA computation technology.

- The original image is encrypted using DNA computation and DNA complementary rule.

- First, a secret key is generated using a DNA sequence and modular arithmetic operations.

- Then each pixel value of the image undergoes the encryption process using the key and DNA computation methods.

Fig:3.2.1 Image to be encrypted (compressed image)

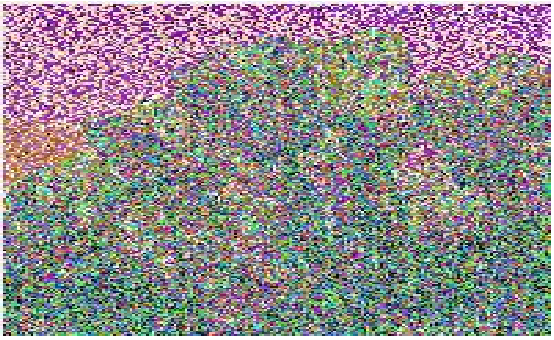

Fig:3.2.2 Image after encryption

3.3 DECRYPTION OF IMAGE

The encrypted image is decrypted using DNA algorithm in reverse order.

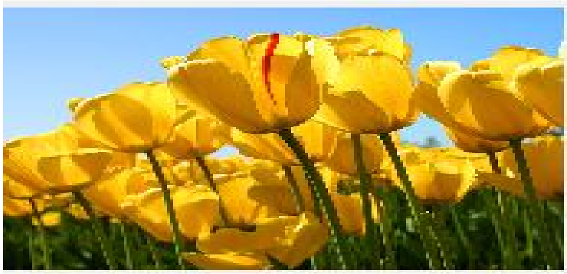

Fig:3.3.1 Decrypted image

3.4HISTOGRAMS OF IMAGE

- An image–histogram illustrates how pixels in an image are distributed at each color intensity level.
- The histogram of original image, encrypted image and decrypted image are plotted.
- Histogram of encrypted image is uniform in nature significantly different from original image histogram.
- Hence any statistical attack is unlikely in this proposed encryption technique.

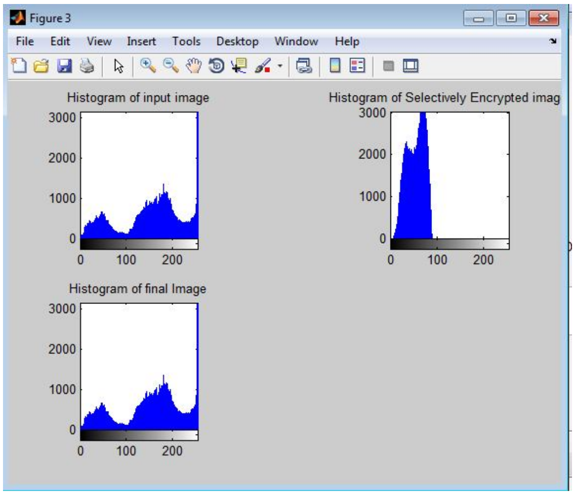

Fig: 3.4.1Histograms of image

4.ALGORITHMS AND TECHNIQUES

A. Compression Algorithm :

Step 1 : Select image with compression level and number of iterations for compression.

Step 2: With image dimensions (2 D).

Iterate for colour channels (Red, Green and Blue)

i.e. for both rows and column of image matrix.

Step 3: Each channel is compressed along with the specified compression level and iteration specified.

Step 4: After the simplified construction of a new varied compressed matrix is created for the specified channel.

Step 5: The count of zeros in the matrix is performed and utilized for compression percentage.

Step 6: The image of compressed status is returned back in matrix form for reconstruction

i.e. from matrix from 2A a normal image (with image compression)

B. Encryption algorithm

Step 1: The further step involves of using the compressed image for encryption using DNA algorithm.

Step 2: The image size and the percentage of key for encryption is given for processing.

Step 3: The image is encrypted using operations such

(i) DNA

(ii) XOR of bits

(iii) Key(s) variant generation

(iv) Integration of all key variants into a single key for decryption.

Step 4: The distorted image after the application of the algorithm is again reconstructed and put to display in its present state (i.e. encrypted state).

Step 5: With further continuation of the process, the public key is acquired and image with encrypted state is read back into 2 D matrix and decrypted back & its original form with key remaining the same.

Step 6: USP :- Time taken calculation

:- Histogram generation for graphical analysis

:- Compression % at various level of iteration

:- Distortion % being the least.

5.CONCLUSION

A novel image encryption algorithm based on Haar wavelet transformation and DNA technique is proposed here. The security analysis and simulation experimental results show that the encryption algorithm is efficient, has large key space, easy to be realized, and is depends upon the secret key.

This DNA algorithm can also resist exhaustive attacks and statistical analysis. Our DNA algorithm does not have complex biological operations that are used in traditional DNA cryptography. It makes use of DNA subsequence operation that is based on horizontal correlation. The adjacent pixels of original image have high may lead to a bit high horizontal correlation. If we change the lengths of DNA subsequence's from each bit-plane then it can improve the horizontal correlation.

To further improve the security of our images over any network we can make use of more complex biological operations, it can make encryption process unbreakable but it also increase the time of encryption and decryption.

REFERENCES

[1] Mohammad Ali Bani Younes and Aman Jantan, “Image Encryption Using Block-BasedTransformation Algorithm”, IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.

[2] Ch. Samson and V. U. K. Sastry , “ An RGB Image Encryption Supported by Wavelet-based Lossless Compression”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3, No. 9, 2012.

[3]Nidhi Sethi, Ram Krishna and Prof R.P. Arora, “Image Compression Using Haar Wavelet Transform”, Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online).

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

[5] Deepika Sharma and Nidhi Sethi,. “A NOVEL METHOD OF IMAGE ENCRYPTION USING LOGISTIC MAPPING” Nidhi Sethi et al. / International Journal of Computer Science Engineering (IJCSE) ISSN : 2319-7323 Vol. 1 No.02 November 2012.

[6]Sandip Vijay and Nidhi Sethi, “Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique”, Conference on Advances in Communication and Control Systems 2013 (CAC2S 2013)

[7] Andrea Gavlasov´a, Aleˇs Proch´azka, and Martina Mudrov´, “WAVELET BASED IMAGE SEGMENTATION”, Simulation and Modeling (ICGSM'2012) July 28-29, 2012 Pattaya (Thailand).

[8] Qiang Zhang, Xianglian Xue, and XiaopengWei, “A Novel Image Encryption Algorithm Based on DNA Subsequence Operation”, The Scientific World Journal
Volume 2012, Article ID 286741, 10 pages doi:10.1100/2012/286741.

[9] J. M. Liu, S. S. Qiu, F. Xiang, and H. J. Xiao, “A cryptosystem based on multiple chaotic maps,” in Proceedings of the International Symposium on Information Processing (ISIP ’08) and International Pacific Workshop on Web Mining and Web- Based Application (WMWA ’08), vol. 99, pp. 740–743, May 2008.

[10] G. Jakimoski and L. Kocarev, “Analysis of some recently proposed chaos-based encryption algorithms,” Physics Letters A, vol. 291, no. 6, pp. 381–384, 2001.

[11] Ms. Sonam Malik and Mr. Vikram Verma, “Comparative analysis of DCT, Haar and Daubechies Wavelet for Image Compression”, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012).

[12] Grasha Jacob and A. Murugan, “ DNA based Cryptography: An Overview and Analysis,” Int. J. Emerg. Sci., 3(1), 36-42, March 2013 ISSN: 2222-4254 © IJES.

[13] Hamid R. Rabiee, R. L. Kashyap1 and H. Radha2, “MULTIRESOLUTION IMAGE COMPRESSION WITH BSP TREES AND MULTILEVEL BTC”, IEEE ICIP’95, Washington D.C., October 1995.

[14] Andrew B. Watson, “Image Compression Using the Discrete Cosine Transform”, Mathematica Journal, 4(1), 1994, p. 81-88.

[15] PETER J. BURT, MEMBER, IEEE, AND EDWARD H. ADELSON, “The Laplacian Pyramid as a Compact Image Code”, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. COM-3l, NO. 4, APRIL 1983.

[16] Uli Grasemann and Risto Miikkulainen, “Effective Image Compression using Evolved Wavelets”, GECCO’05, June 25–29, 2005, Washington, DC, USA. Copyright 2005 ACM 1595930108/05/0006.

[17] P. Raviraj and M.Y. Sanavullah, “The Modified 2D-Haar Wavelet Transformation in Image Compression”, Middle-East Journal of Scientific Research 2 (2): 73-78, 2007
ISSN 1990-9233.

[18] Anusorn Jitkam and Satra Wongthanavasu, “Image Compression using Modified Haar Wavelet-Base Vector Quantization”, ECTI TRANSACTIONS ON COMPUTER AND INFORMATION TECHNOLOGY VOL.3, NO.1 MAY 2007.

[19] Ashish Gehani, LaBean, T.H., and John H. Reif, “DNA-based Cryptography”, Proceedings of DIMACS Workshop V on DNA Based Computers, American Mathematical Society, 1999. vol. 54. , pp 233–249.

[20] Borda M.E, Tornea O, “DNA secret writing Techniques” IEEE conferences 2010

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