A NOVEL IMAGE ENCRYPTION BASED ON DNA SUBSEQUENCE OPERATION WITH COMPRESSION USING HARR TRANSFORM

[1]Rohit Malik, [2] Sunaina Malik
[1]HOD,Computer Science and Engg, Manda Institute of Technology,Bikaner
[2]Asst Professor, Computer Science and Engg, Manda Institute of Technology,Bikaner

***Abstract*—Image encryption is the process of transforming the information to ensure its security. Different type of data demand different aspects, and techniques to protect the confidentiality of data from unauthorized access. The large size of image compared to that of the text demands more time for the encryption process. Image encryption has applications in internet communication, multimedia systems, medical imaging, military communication, etc. The aim of our work is to obtain an effective cipher and high-quality image compression to achieve both security against unauthorized access during data transmission through an unsecured channel and high compression to allow for a low transmission rate. We used an efficient algorithm based on DNA subsequences to encrypt the low subband of the image. For the compression, we used Haar wavelet transform, and the results were highly satisfactory; this method allowed us to achieve a perfect reconstruction with a good PSNR. In our work the image encryption is supported by image compression technique. The image is compressed and then encrypted in order to get a high-quality compressed image for enhanced encryption. With the experiment results we found 100% efficiency in image compression and a satisfactory result in image encryption and decryption.**

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

1. INTRODUCTION

As computers have become more and more powerful, the temptation to use digital images has become irresistible. Digital images require large amounts of memory to store and, when retrieved from the internet, can take a considerable amount of time to download. Compression makes it possible for creating file sizes of manageable, storable and transmittable dimensions. A 4 MB image will take more than a minute to download using a 64kbps channel, whereas, if the image is compressed with a ratio of 10:1, it will have a size of 400KB and will take about 6 seconds to download. One of the important factors for image storage or transmission over any communication media is the image compression. Image compression [1] is of two types: lossy or lossless. In lossless compression, the recovered data is identical to the original, whereas in the case of lossy compression the recovered data is a close replica of the original with minimal loss of data. Lossless compression can be used for text, medical images and legal documents etc. whereas lossy compression is used for natural images, speech signals etc. With rapid developments in the multimedia and communications industry, a major challenge is to protect the confidentiality of such images in wired and wireless networks. The most effective method is to encrypt the image so that only authorized entities with the key can decrypt them. The limitations [6] on using encryption for securing images are: (1) Perceptual quality control - An image encryption algorithm can be used to intentionally degrade the quality of the image. However, the degradation must be visually unperceivable, (2) Real-time constraint - In many multimedia applications, very efficient encryption and decryption algorithms are needed to access images in a real-time environment.

Fig: 1.1 The process of encryption and decryption.

Image encryption is the process of transforming the information to ensure its security. Different type of data demand different aspects, and techniques to protect the confidentiality of data from unauthorized access.

With the rapid development of DNA computing, DNA cryptography, as a new field, has come into being. DNA cryptography provides higher security to data, in this technique plain text message is converted in to DNA strength by using DNA sequence. A method for hiding message in DNA microdots was proposed by Clelland et al. [8]. Clelland used DNA microdots to hide message to implement the protection of information. For instance, letter A is expressed as DNA sequence GGT by complex

biological operation

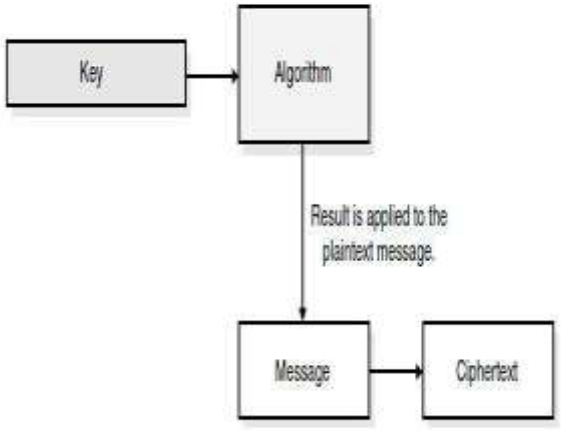


Fig: 1.2 The key is inserted into the mathematical algorithm and the result is applied to the message, which ends up in cipher text.

In our proposed scheme, we do not use biological operation to implement image encryption, but adopt the rule of DNA subsequence operation such as truncation operation, deletion operation, transformation operation and so forth, to scramble the location and the value of pixel point from the image. 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 secret. 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 Random Pixel Permutation by Chaotic Mapping [1]: In this paper, a new image encryption algorithm is proposed using random pixel permutation based on chaos logistics maps and prime modulo multiplicative linear congruential generators (PMMLCG). The pixel transformation results in the encryption scheme being resistive to cryptanalytic attacks. Simulation results show high sensitivity to key, plaintext and cipher text changes.

B) Image [2] Encryption Algorithm Based on A New Combined Chaotic System: In this paper, we introduce a new combined chaotic system, which shows better chaotic behaviors than the traditional ones. Applying this chaotic system to image processing, a new image encryption algorithm is introduced based on the confusion and diffusion in encryption procedure. Experimental results show that the proposed algorithm has a higher security level and excellent performance in image encryption.

C) 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.

D) **An [4] 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.

E) Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation [5]:

In this paper, a highly efficient image encryption-then-compression (ETC) system was designed , where both lossless and lossy compression are considered. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. Also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only slightly worse, in terms of compression efficiency, than the state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs.

F) Image encryption method using logistic mapping:
It introduced an advance method to develop secure image-encryption techniques with the help of [6] 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.

G) A Secured Image with Pseudorandom Permutation Using longer bit with Chaotic Maps:
In this paper, a new image secured algorithm using a large pseudorandom permutation which is combinatorial generated from small permutation matrices based on chaotic maps. The proposed algorithm [7] uses longer pseudorandom bits for encryptions. The random-like nature of chaos is effectively spread into encrypted images by using the permutation matrix. This shows that the proposed encryption scheme provides comparable security with that of the conventional image encryption schemes based on Baker map or Logistic map.

[H] Image Encryption scheme with a pseudorandom permutation based on chaotic maps [8]: In this paper, new image encryption algorithm using a large pseudorandom permutation which is combinatorically generated from small permutation matrices based on chaotic maps.

I) Image segmentation based on wavelet transformation: [9] 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.

J) A Novel Image Encryption Algorithm [10] 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 work is to first compress the image so that we can send it over the network quickly and encrypt it so that we can transmit it over any network securely and safely. 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.

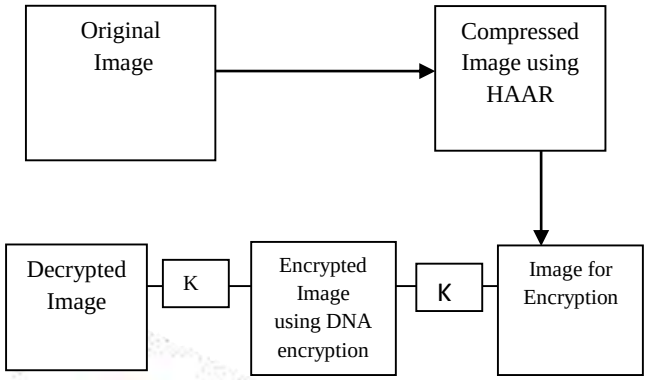


Fig: 3.1.1 Basic Architecture of DNA encryption using compression by Haar wavelet transform

Wavelet transform divides the information of an image into approximation and detail sub-signals. The approximation sub-signal shows the general trend of pixel values and other three detail sub-signals show the vertical, horizontal and diagonal details or changes in the images. If these details are very small (threshold) then they can be set to zero without significantly changing the image. The greater the number of zeros the greater the compression ratio. If the energy retained (amount of information retained by an image after compression and decompression) is 100% then the compression is lossless as the image can be reconstructed exactly. This occurs when the threshold value is set to zero, meaning that the details have not been changed. If any value is changed then energy will be lost and thus lossy compression occurs. As more zeros are obtained, more energy is lost. Therefore, a balance between the two needs to be found out.

The first DWT 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 basic functions that represents the input function in the most efficient way.
- Thus wavelets are able to provide a great value of compression and are therefore very popular in the field of image and signal processing.

3.2. HAAR WAVELET TECHNIQUE

A. Haar Wavelet Transform

To understand how wavelets work, let us start with a simple example. Assume we have a 1D image with a resolution of four pixels, having values [9 7 3 5]. Haar wavelet basis can be to represent this image by computing a wavelet transform. To do this, first the average of the pixels together, pair wise, is calculated to get the new lower resolution image with pixel values [8 4]. Clearly, some information is lost in this averaging process. We need to store some detail coefficients to recover the original four pixel values from the two averaged values. In our example, 1 is chosen for the first detail coefficient, since the average computed is 1 less than 9 and 1 more than 7.. This single number is used to recover the first two pixels of our original four-pixel image. Similarly, the second detail coefficient is -1, since 4 + (-1) = 3 and 4 - (-1) = 5. Thus, the original image is decomposed into a lower resolution (two-pixel) version and a pair of detail coefficients. Repeating this process recursively on the averages gives the full decomposition shown in **Table 3.2:**

Table 3.2: Decomposition to lower resolution and a pair of detail coefficients

Resolution	Averages	Detail Coefficients
4	[9 7 3 5]	
2	[8 4]	[1 -1]
1	[6]	[2]

Thus, for the one-dimensional Haar basis, the wavelet transform of the original four-pixel image is given by [6 2 1 -1]. We call the way used to compute the wavelet transform by recursively averaging and differencing coefficients, filter bank. We can reconstruct the image to any resolution by recursively adding and subtracting the detail coefficients from the lower resolution versions.

B. 2D Haar wavelet transformation

Now, we see how the 2D Haar wavelet transformation is performed. The image is comprised of pixels represented by numbers. Consider the 8×8 image taken from a specific portion of a typical image shown in Fig. 3.2(a). The matrix (a 2D array) representing this image is shown in Fig. 3.2(b).

Now we perform the operation of averaging and differencing to arrive at a new matrix representing the same image in a more concise manner. Let us look how the operation is done. Consider the first row of the Fig. 3.2(b).

Averaging: (64+2)/2=33,(3+61)/2=32, (60+6)/2=33, (7+57)/2=32

Differencing: 64–33 =31, 3–32= –29, 60– 33=27 and 7–32= –25

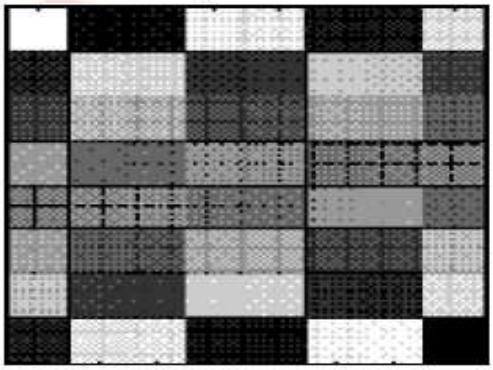


Fig. 3.2.(a). A 8×8 image

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

Fig.3.2.(b). 2D array representing the Fig. 3.2(a)

So, the transformed row becomes (33 32 33 32 31 –29 27 –25). Now the same operation on the average values i.e. (33 32 33 32) is performed. Then we perform the same operation on the averages i.e. first two elements of the

new transformed row. Thus the final transformed row becomes (32.5 0 0.5 0.5 31 –29 27 –25). The new matrix we get after applying this operation on each row of the entire matrix of Fig. 3.2(b) is shown in Fig. 3.2(c). Performing the same operation on each column of the matrix in Fig. 3.2(c), we get the final transformed matrix as shown in Fig. 3.2(d). This operation on rows followed by columns of the matrix is performed recursively depending on the level of transformation meaning the more iteration provides more transformations. Note that the left-top element of the Fig. 3.2(d) i.e. 32.5 is the only averaging element which is the overall average of all elements of the original matrix and the rest all elements are the details coefficients.

32.5	0	0.5	0.5	31	–29	27	–25
32.5	0	–0.5	–0.5	–23	21	–19	17
32.5	0	–0.5	–0.5	–15	13	–11	9
32.5	0	0.5	0.5	7	–5	3	–1
32.5	0	0.5	0.5	–1	3	–5	7
32.5	0	–0.5	–0.5	9	–11	13	–15
32.5	0	–0.5	–0.5	17	–19	21	–23
32.5	0	0.5	0.5	–25	27	–29	31

Fig. 3.2(c). Transformed array after operation on each row of Fig. 3.2(b)

It can be seen that in the final transformed matrix, we find a lot of entries zero. From this transformed matrix, the original matrix can be easily calculated just by the reverse operation of averaging and differencing i.e. the original image can be reconstructed from the transformed image without the loss of information.. Thus, it yields a lossless compression of the image. However, to achieve more degree of compression, we have to think of the lossy compression. In this case, a nonnegative threshold value say ε is set.. Then, any detail coefficient in the transformed data whose magnitude is less than or equal to ε is set to zero. It will increase the number of 0's in the transformed matrix and thus the level of compression is increased. So, ε =0 is used for a lossless compression. If the lossy compression is used, the approximations of the original image can be built up. The setting of the threshold value is very important as there is a tradeoff between the value of ε and the quality of the compressed image. Loosely saying, the compression ratio of the image is calculated by the number of nonzero elements in original matrix: the number of nonzero elements in updated transformed matrix.

Fig. 3.2.(d). Original Image of penguins
Size of original image is : 759 KB (777,835 bytes)

Fig.3.2.(e). Compressed image of the Original Image using Haar wavelet transform. Size of compressed image of penguins is: 69.4 KB (71,080 bytes)

Comparing the sizes of both the original image of Penguins.jpg and the compressed image, PenguinsCmp.jpg of the original image, we can conclude the image is reduced to almost 90% using Haar transform for the compression

3.3 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. 3.3.1. Image Encryption using DNA encryption

3.4 DECRYPTION OF IMAGE

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

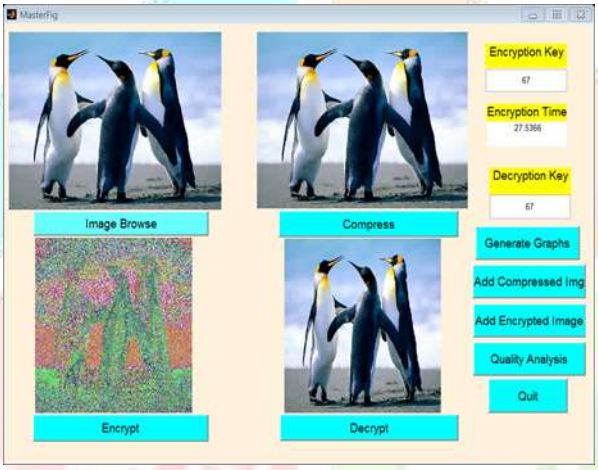


Fig:3.4.1. Image Decryption

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 zero 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.

B. Encryption algorithm

Step 1: The further steps 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

(i) DNA

(ii) XOR of bits

(iii) Generation of variant key(s)

(iv) Integration of variant keys into a single key for decryption.

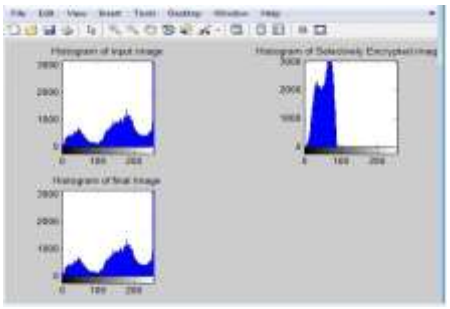
Step 4: The distorted image is reconstructed using the algorithm and displayed in encrypted state.

Step 5: The public key is accquired and image with encrypted state is read back into 2 D matrix and decrypted back and its original form with key remaining the same.

Step 6: USP:- Time taken calculation

:- Histogram generation

:-Compression % at various level of iteration



:-Distortion % being the

3.5. Histograms of image

Fig: 3.5.1. Histogram of Images

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 (2D).

Iterate for colour channels (Red, Green, and Blue) i.e for both rows and column of image matrix.

5. Performance and Results

A. Qualitative Analysis

Qualitative analysis includes perception of the images and the analysis of histogram.

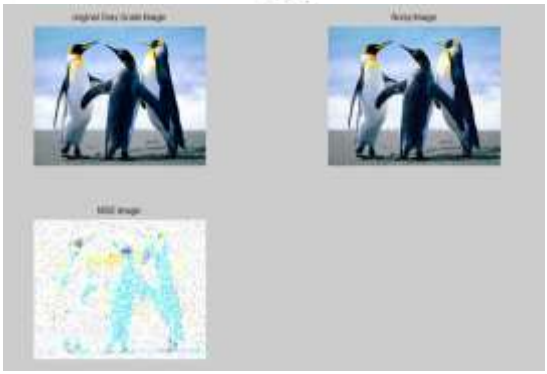
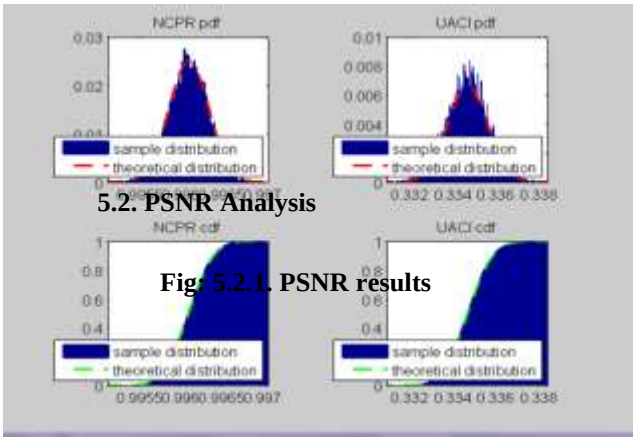


Fig: 5.1. Qualitative analysis result



5.2. PSNR Analysis

Fig: 5.2.1. PSNR results

5.3. NPCR and UACI Analysis

```
The mean square erroe is 56.69
The PSNR = 59.10 The mean square erroe is 55.03
The PSNR = 30.63 The mean square erroe is 30.45
The PSNR = 30.76
```

Fig: 5.3.1. NPCR and UACI results

5. CONCLUSION

In this analysis, we have found that wavelet transform is very powerful and extremely useful for compressing data such as images. The proposed a new image encryption algorithm based on DNA sequence addition. In this proposed scheme, the pixel grey values of the original image are scrambled by DNA sequence addition operation and DNA complement operation completely. Through the experiment result and security analysis, we find that our algorithm has better encryption effect, larger secret key space and high sensitive to the secret key. Furthermore, the proposed algorithm also can resist most known attacks, such as exhaustive attack, statistical attack and differential attack. All these features show that our algorithm is very suitable for image encryption.

REFERENCE

[1] Dr.K.Bhoopathy Bagan, "Image Encryption Using Random Pixel Permutation by Chaotic Mapping", 2012 IEEE symposium on Computers and Informatics.

[2] C.L. Philip Chen, Tong Zhang, Yicong Zhou, "Image Encryption Algorithm Based on A New Combined Chaotic System", 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea

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

[4] 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.

[5] Jiantao Zhou, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", *Member, IEEE*, Xianming Liu, *Member, IEEE*, Oscar C. Au, *Fellow, IEEE*, and Yuan Yan Tang, *Fellow, IEEE*, IEEE Transactions on information forensics and security, vol. 9, no. 1, January 2014.

[6] Deepika Sharma and Nidhi Sethi,. "A NOVEL METHOD OF IMAGE ENCRYPTION USING LOGISTIC MAPPING" Nidhi Sethi et al. / International Journal of Computer Science Engineering

[7]"A Secured Image with Pseudorandom Permutation Using longer bit with Chaotic Maps", by Sumit Oswal, Sandeep Rai, International journal of Digital Signal and Image Processing (IJDSIP)Vol. 1, No. 1(September 2013)

[8] "**Image Encryption scheme with a pseudorandom permutation based on chaotic maps" by** Ji Won Yoon, Hyoungshick Kim, University of Oxford, Parks Road, Oxford, UK, " Commun Nonlinear Sci Numer Simulat (2010)"

[9] Andrea Gavlasov´a, Ale˘s Proch´azka, and Martina Mudrov´, "WAVELET BASED IMAGE SEGMENTATION", Simulation and Modeling (ICGSM'2012) July 28-29, 2012 Pattaya (Thailand).

[10] 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

[11] Namita Tiwari, Dept, "Image Encryption using Pseudo Random Number Generators", International Journal of Computer Applications (0975 – 8887) Volume 67– No.20, April 2013.

[12] Prof. Avinash Ghorpade, Priyanka Katkar, "Image Compression Using Haar transform and Modified Fast Haar Wavelet Transform", IJSTR, 2014.

[13] K.P. Soman, K.I. Ramachandran, "Insight into Wavelets from theory to practice", Second edition, PHI, 2006. (IJCSE) ISSN : 2319-7323 Vol. 1 No.02 November 2012.

[14] S. Mallat, "A Wavelet Tour of Signal Processing", (AcademicPress, 1999).

[15] VinodPatidar , N.K. Pareek , K.K. Sud, " A new substitution–diffusion based image cipher using chaotic standard and logistic maps", University Computer Centre, VigyanBhawan, New Campus, M.L.S. University, Udaipur 313 002, Rajasthan, India.

[16] Qiang Zhang, Xianglian Xue, and XiaopengWei, "An Image Encryption Algorithm Based on DNA Sequence Addition Operation", 978-1-4244-3867-9/09/$25.00 ©2009 IEEE.

[17] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," Nature, vol. 399, no. 6736, pp. 533–534, 1999.

[18] Yashaswita R. Bhoir, R.Mathangi, "DNA cryptography with binary strands", Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India.

[19] Shihua Zhou, Qiang Zhang, Xiaopeng Wei, "Image Encryption Algorithm Based on DNA Sequences for the Big Image", 978-0-7695-4258-4/10 $26.00 © 2010 IEEE, DOI 10.1109/MINES.2010.188, 2010 International Conference on Multimedia Information Networking and Security.

[20] Qian Wang, Qiang Zhang, Xiaopeng Wei, "Image Encryption Algorithm based on DNA Biological Properties and Chaotic Systems", Key Laboratory of Advanced Design and Intelligent Computing (Dalian university)Ministry of Education Dalian, 116622, China, 978-1-4244-6439-5/10/$26.00 ©2010 IEEE.

[21] Nidhi Sethi, Deepika Sharma, "A novel method of image encryption using logistic mapping", International Journal of Computer Science Engineering (IJCSE), ISSN : 2319-7323 Vol. 1 No.02 November 2012.

[22] Kamrul Hasan Talukder, Koichi HaradaI, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", IAENG International Journal of Applied Mathematics, February 2007.