ISSN:0975-9646

Image Encryption and Compression using HAAR and COIFLET Wavelet Transform

Navita Palta[#1], Neha Sharma[*2]

[#1]*M.Tech Student,*
Punjab Technical University,
CEC Landran

[*2]*Assistant Professor,*
CEC Landran,
Punjab Technical University

ABSTRACT: **There is rapid development in the multimedia and network technologies where the privacies and securities become the important issues in the multimedia which transmitted openly over the network. In this work, we design and implement an image with encryption and compression system, in which the lossy compression is considered. The proposed operated scheme for image encryption with random permutation method which is shown to be able to provide reasonably high level of security[1]. Here a new image compression algorithm is implemented using the HAAR and COIFLET Wavelet Transform that can be used to efficiently compress the encrypted image. More notably, the approach applied for compression to encrypted image that proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Entropy, Bit Error Rate(BER).**

Keywords: **Image Encryption, Image Compression, HAAR Wavelet and COIFLET Wavelet Transform.**

I. INTRODUCTION

The security of multimedia becomes more important, since multimedia data are transmitted over open networks more frequently[10]. Typically, reliable security is necessary to content protection of digital images and videos. Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. For example, real-time encryption of an image using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level, this can be achieved using selective encryption that leaves some perceptual information after encryption.

A marked progress built in the field of image compression and its application in various branches of engineering. Image compression is associated with separating redundant information of image data and it is a solution which associated with storage and data transmission problem of huge amounts of data for digital image[18]. Application of Image transmission which includes the broadcast television, remote sensing by satellite and also other long distance communication systems. This requires the image storage for several purposes like document, medical images, MRI and radiology, motion pictures etc. These applications are based on image compression.

1.1 Benefits of Image Compression

- It provides a cost savings associated with sending less data over switched telephone network where cost of call is really usually based upon its duration.
- It helps in reducing storage requirements and overall execution time.
- It also reduces the probability of transmission errors as less bits are transferred.
- It helps in providing security against illegal monitoring.

The above mentioned benefits and requirements of image encryption and image compression. Here, combining the both techniques so that an image can be transmitted over a network with complete security and also taking small storage space.

1.2 Encryption and Compression System

Consider an application scenario in which a content owner Alice wants to securely and efficiently transmit an image to a recipient Bob.

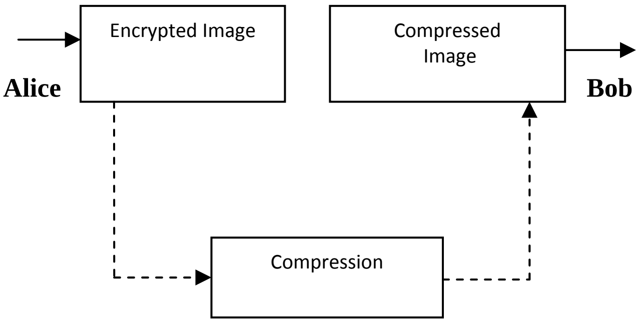

Figure 1: Encryption and Compression System

In the above Figure 1 Encryption-Compression Scheme is represented in which image is first encrypted using random permutation method as encryption technique and then the encrypted image is compressed using haar and coif let wavelet transform.

II. Techniques Used

There are two main techniques that are used in proposed work to enhance the results. These techniques are explained below:-

2.1. HAAR Wavelet

The HAAR wavelet is a sure arrangement of capacities which is presently perceived as the first known wavelet. HAAR utilized these capacities to give an illustration of a countable ortho-ordinary framework for the space of square vital capacities on the genuine line[2]. The investigation of wavelets and the expression "wavelet" did not come until much later. The HAAR wavelet is also the simplest wavelet.

The HAAR wavelet's function ψ (t) can be described as:

$$\psi(t) = \begin{cases} 1 \\ -1 \\ 0 \end{cases}$$

$0 \leq t < \frac{1}{2}$,

$1/2 \leq t < 1$, otherwise

Scaling function φ (t) can be described as:

$$\phi(t) = \begin{cases} 1 \\ 0 \end{cases}$$

$0 \leq t < 1$, otherwise

Wavelets are numerical capacities that were created by researchers working in a few separate fields with the end goal of sorting information by its recurrence. At that point the Translated information can be sorted at a determination which matches its scale. At distinctive levels, the Studying information takes into consideration the advancement of a more finish picture. By this, both little highlights and extensive highlights are discernable in light of the fact that they are concentrated on independently. After that, the wavelet change is not Fourier-based and subsequently wavelets improve employment of taking care of discontinuities in information[2]. The HAAR wavelet works on information by computing the totals and contrasts of components which are neighbouring. The HAAR wavelet operates first on adjacent horizontal elements and after that on adjacent vertical elements. The HAAR transform is computed by using the following:

$$1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Following are the properties of Haar transform:

- No need for multiplications. It requires only additions and there are many elements with zero value in the Haar matrix, so the computation time is short. It is faster than Walsh transform, whose matrix is composed of +1 and −1.
- Input and output length is the same. However, the length should be a power of 2, i.e. $N=2^k$, K €N. 3. It can be used to analyse the localized feature of signals. Due to the orthogonal property of the Haar function, the frequency components of input signal can be analyzed.

2.2 COIFLET Wavelet

Coiflets are the wavelets designed by Ingrid Daubechies. These are the discrete wavelets which are made at the request of Ronald Coifman for having scaling functions along with vanishing moments. The wavelets are symmetric in nature and its function have N/3 vanishing moments and scaling functions N/3-1 which are used in different applications with the help of Calderon-Zygmund Operators.

The normalization of both scaling function (low-pass filter) and the wavelet function (High-Pass Filter) is done by a factor $1 - \sqrt{2}$. There are some coefficients for the scaling functions for C6-30. The wavelet coefficients are obtained by reversing the order of the scaling function coefficients and then reversing the sign of every second[8].

Mathematically, this looks like $B_K= (-1)^K C_{N-1-K}$ where k is the coefficient index; B is a wavelet coefficient and C is a scaling function coefficient. N is the wavelet index, i.e 6 for C6.The 2N moments of wavelet functions are equal to 0 and the 2N-1 moments of scaling functions are equal to 0. The two functions have a support of length 6N-1[3]. F= coifwavf(W) returns the scaling filter associated with the Coiflet wavelet specified by the string W where W = 'coifN' whereas the values of N are 1, 2, 3, 4 or 5[8].

III. Proposed Work

Following are the steps used to make an efficient image encryption and compression system.

Phase 1: Take an input original image.

Phase 2: Perform filtering on the input image in order to remove noise.

Phase 3: Perform encryption process on it in order to convert it into unreadable format via random permutation and prediction error clustering.

Phase 4: Finally Haar and COIFLET wavelet transform with encryption algorithm are applied on the input image.

Phase 5: Compare Obtained results with previous work.

Firstly an input image is taken. Then prediction values of an image are predicted via GAP. These predicted values mapped up and different clusters are made containing all predicted values. After that reshape the clusters into blocks then apply random permutation technique in order to secure the image. Then assembles them to make an encrypted image. Then for compression is done for that encrypted image is taken, decompose it then reconstructs the coefficients of image and convert it into matrix.

After that take the previous output as an input into coiflet transform. Compute its scaling function and then display the compressed image. At last analyse and compare the results On the basis of mean square error(MSE), Entropy, Bit Error Rate(BER), Compression Ratio(CR) and Peak signal noise ratio(PSNR).

The following diagram depicts the steps of proposed work in which the encryption and compression are the two main tasks. These steps clearly explains the way methods are operated on image encryption and compression system using Haar and Coiflet Wavelet transform.

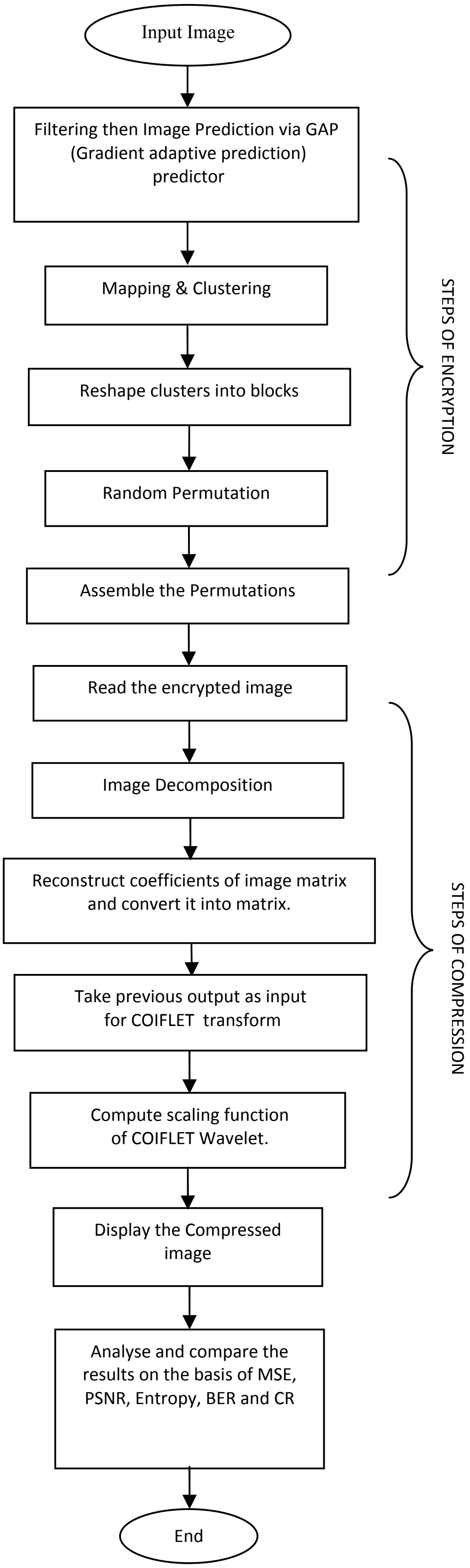
Input Image
Filtering then Image Prediction via GAP (Gradient adaptive prediction) predictor
Mapping & Clustering
Reshape clusters into blocks
Random Permutation
Assemble the Permutations
STEPS OF ENCRYPTION
Read the encrypted image
Image Decomposition
Reconstruct coefficients of image matrix and convert it into matrix.
Take previous output as input for COIFLET transform
Compute scaling function of COIFLET Wavelet.
STEPS OF COMPRESSION
Display the Compressed image
Analyse and compare the results on the basis of MSE, PSNR, Entropy, BER and CR
End

Figure 2: Flow chart of proposed work

IV. Parameters Used

There are some parameters given which are useful in our implementation.

4.1. CR(Compression Ratio)

The compression ratio i.e. the size of the compressed image compared to that of the uncompressed image. Still images are often compressed at 10:1, but the quality loss is more noticeable, especially on closer inspection.

$$C_R = n1/n2$$

where n1 is the size of original image and n2 is the size of compressed image.

4.2. MSE (Mean Square Error)

MSE is essentially a signal fidelity measure. The goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of similarity/fidelity or, conversely, the level of error/distortion between them. Usually, it is assumed that one of the signals is a pristine original, while the other is distorted or contaminated by errors. The MSE between the signals is given by the following formula:

$$MSE = \frac{1}{M * N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) \quad - F(x,y)]$$

where MxN is the size of image, f(x,y) is the original image and F(x,y) is the compressed image.

4.3. PSNR (Peak Signal to Noise Ratio)

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g. for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not.

The PSNR values can be obtained using following formula-

$$PSNR = 10 \log_{10}(255/(\sqrt{MSE}))^2$$

MSE and PSNR are most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of reconstruction quality.

4.4 Entropy

Image entropy is the quality which is used to describe the 'business ' of an image i.e. the amount of the information which must be coded for compression algorithm. Low entropy images, such as those contain lot of black sky, have very little contrast and large runs of pixels with the same or similar DN values. An image that is perfectly flat will have entropy of zero. Consequently, they can be compressed to a relative small size. On the other hand, high entropy such as image of heavily cratered areas on the moon has great deal of contrast from one pixel to the next and consequently cannot be compressed as much as low entropy image.

$$ENTROPY = -\sum Pj \log_2 Pj$$

4.5 Bit Error Rate (BER)

As the name implies, a bit error rate is defined as the rate at which errors occur in the transmission system. This can be directly translated into the number of errors that occur in a string of a stated numbers of bits. If the medium between the transmitter and receiver is good and the signal to noise ratio high, then the bit error rate will be very small - possibly insignificant and having no noticeable effect on the overall system However if the noise can be detected, then there is chance that the bit error rate will need to be considered mapped against each other on a graph known as ROC curve. ROC curve are used in biometric to measure the accuracy of a biometric matcher.

Bit Error Rate (BER) $= \frac{Number\ of\ bits\ received\ in\ error}{Total\ number\ of\ bits\ transmitted}$

V. Results And Discussion

Following are the results on different images of Lossy compression performance when size=150*150 pixels. Here all the below bar graphs shows that results of present work are better than previous work For example, in man.jpeg. MSE reduced from 2.98 to 2.54, PSNR changes from 49.91 to 52.76 , Entropy changes from 7.26 to 7.72 ,BER reduced to 2.42 from 2.85 and CR increases from 1.38 to 1.64.

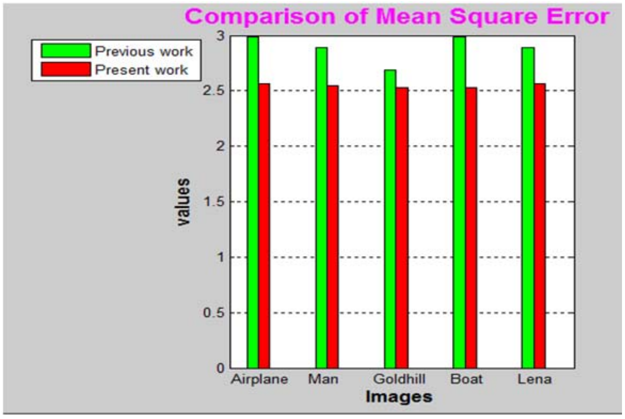

Figure 3: Comparison of MSE between previous and present work

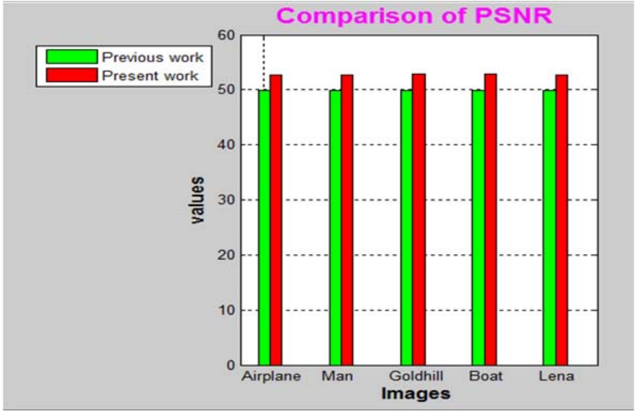

Figure 4: Comparison of PSNR between previous and present work

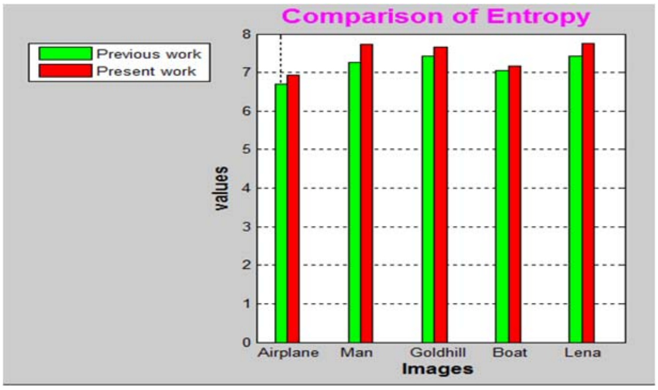

Figure 5: Comparison of Entropy between previous and present work

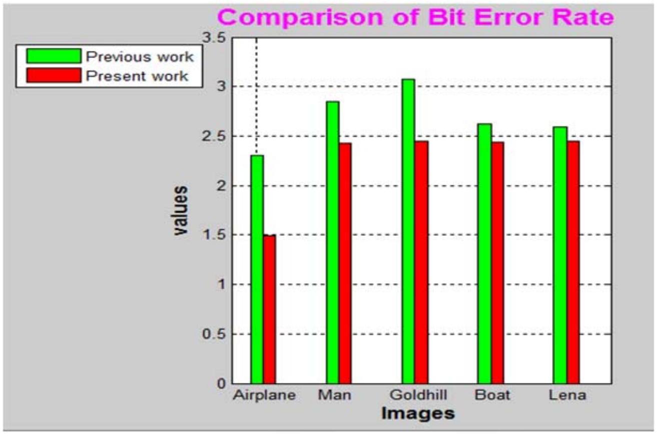

Figure 6: Comparison of BER between previous and present work

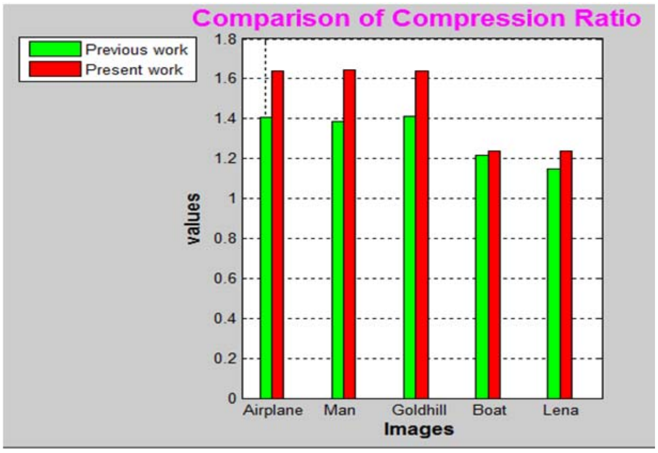

Figure 7: Comparison of CR between previous and present work

Following are the other results of Lossy compression performance when size=200*200

Following are the results of different images of Lossy compression performance when size=200*200 pixels. It is observed that with increase in size of an image results starts decreasing. For example, In man.jpeg, MSE changes to 3.0496, PSNR changes to 52.7644 , Entropy changes to 7.6010 ,BER increased to 2.5668 and CR remains same.

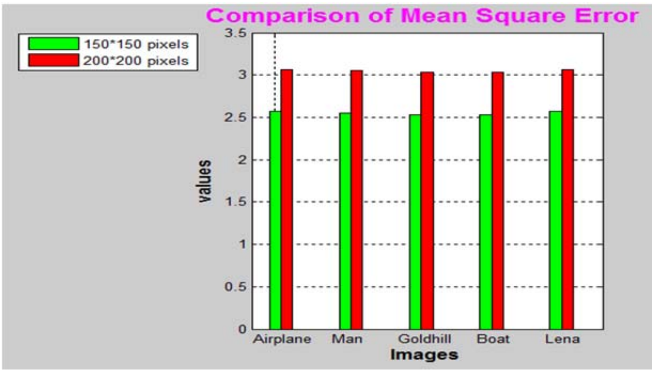

Figure 8: Comparison of MSE between 150*150 pixels and 200*200 pixels

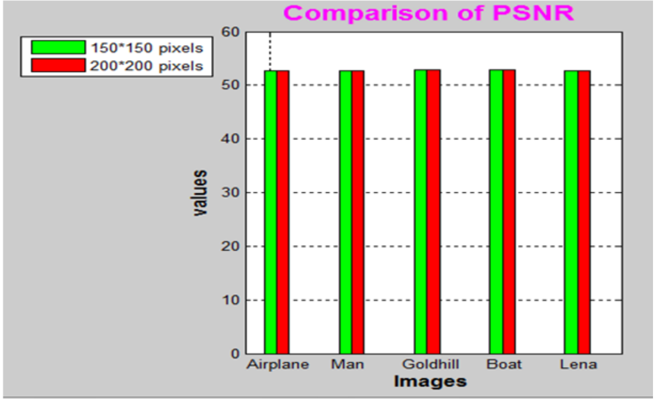

Figure 9: Comparison of PSNR between 150*150 pixels and 200*200 pixels

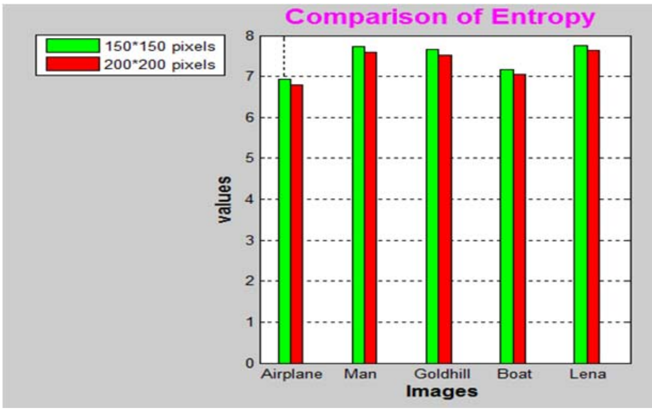

Figure 10: Comparison of Entropy between 150*150 pixels and 200*200 pixels

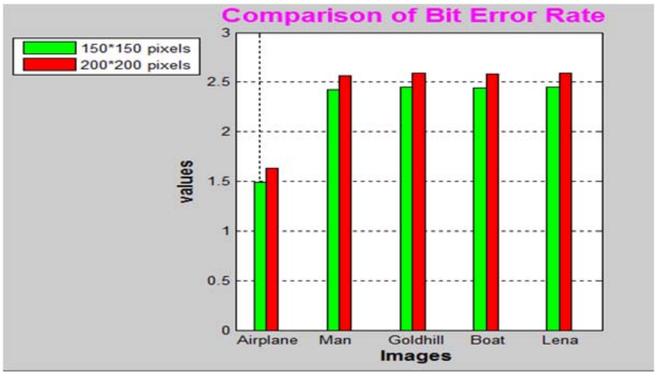

Figure 11: Comparison of BER between between 150*150 pixels and 200*200 pixels

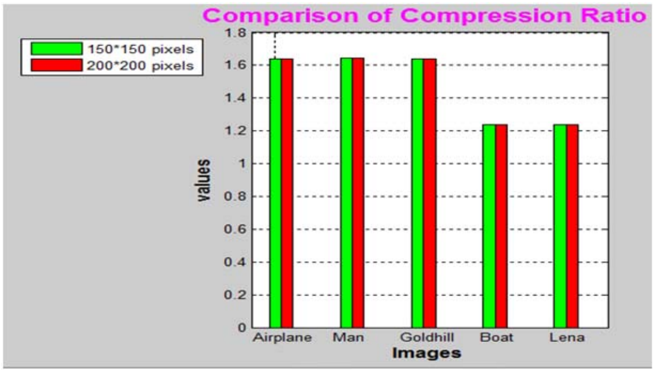

Figure 12: Comparison of CR between between 150*150 pixels and 200*200 pixels

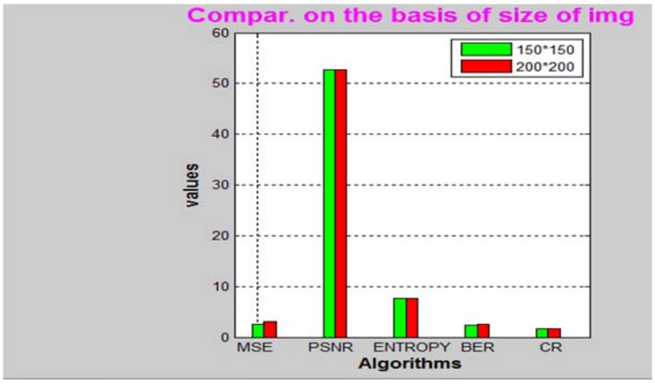

Figure 13: Comparison of all parameters with change in size of an image named man.jpeg .

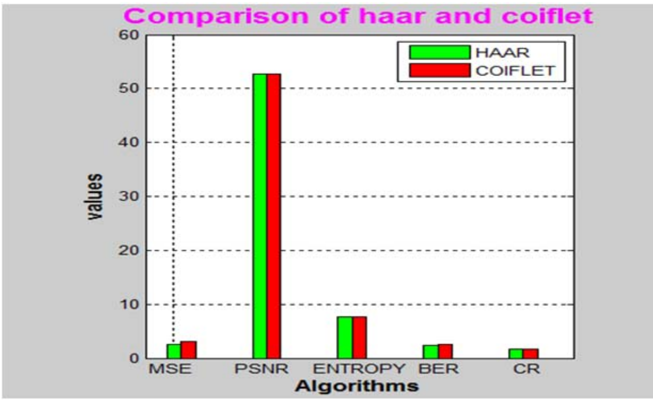

Figure 14: Comparison of haar and coiflet wavelet transform on an image image named man.jpeg .

Table 1: Comparison of Lossy compression performance when size=150*150 pixels

IMAGES	MSE	PSNR	ENTROPY	BER	CR
Airplane	2.56	52.6	6.92	1.49	1.64
Barbara	2.54	52.7	7.93	2.44	1.64
Boat	2.53	52.8	7.16	2.44	1.24
Bridge	2.49	52.1	8.00	3.44	1.64
Goldhill	2.53	52.8	7.64	2.44	1.63
Harbor	2.56	52.6	7.63	2.49	1.64
Lena	2.56	52.6	7.74	2.44	1.23
Man	2.54	52.7	7.72	2.42	1.64
Peppers	2.52	51.9	7.99	2.43	1.64
Tank	2.54	52.7	6.40	2.42	1.24
Average	2.53	52.5	7.51	2.44	1.51

Table 2: Comparison of Lossy compression performance when size=200*200 pixels

IMAGES	MSE	PSNR	ENTROPY	BER	CR
Airplane	3.06	52.6	6.80	1.63	1.64
Barbara	3.04	52.7	7.81	2.58	1.64
Boat	3.03	52.8	7.04	2.58	1.24
Bridge	2.99	52.0	7.88	3.58	1.64
Goldhill	3.03	52.8	7.52	2.58	1.63
Harbor	3.06	52.6	7.51	2.63	1.64
Lena	3.06	52.6	7.62	2.58	1.23
Man	3.04	52.7	7.60	2.56	1.64
Peppers	3.02	51.8	7.87	2.57	1.64
Tank	3.04	52.7	6.28	2.56	1.24
Average	3.03	52.5	7.39	2.58	1.51

VI. Conclusion

This research work designs an efficient image for Encryption and Compression system. Framework of this proposed work, has been achieved the image encryption by random permutation. Therefore, highly efficient compression of encrypted image realized by a new image compression algorithm of Haar and COIFLET wavelet transform. The Experimental results shows that Haar wavelet is better than coiflet wavelet as results are better in case of Haar. It also shows that after integrating both techniques in order to make two tier system, with change in size of an image results will decrease. Thus, when size is 150*150 pixels results are good but with change in size to 200*200 pixels results ends in lossy compression as results will decrease. Moreover, the images results in terms of all parameters values are better than the previous one. Here, the Better all parameters value indicates the obtained image is of higher quality. For the future, it can be extended with the same technique or some other different techniques by applying different transforms to cover image and thus robustness of algorithm can be verified.

Acknowledgement

Thanks to my Guide and family member who always support, help and guide my during my dissertation. Special thanks to my father who always support my innovative ideas.

References

[1] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, “Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation”, IEEE Trans. Inf. Forensics Security, vol. 9, issue 1, January 2014.

[2] R. Mehala and K. Kuppusamy, “A New Image Compression Algorithm using Haar Wavelet Transformation”, International Journal of Computer Applications(0975-8887), International Conference on Computing and Information Technology, 2013.

[3] Sandeep Kaur, Gaganpreet Kaur, Dr.Dheerendra Singh, “Comparative Analysis of Haar and Coiflet Wavelets Using Discrete Wavelet Transform in Digital Image Compression”, International Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 3, Issue 3, May-Jun 2013, pp.669-673.

[4] J. Zhou, X. Wu, and L. Zhang, “l_2 restoration of l_∞-decoded images via soft-decision estimation”, IEEE Trans. Imag. Process. vol. 21, issue 12, Dec. 2012.

[5] X. Zhang, G. Feng, Y. Ren, and Z. Qian, “Scalable coding of encrypted images”, IEEE Trans. Imag. Process, vol. 21, issue 6, June 2012.

[6] Komal D Patel, Sonal Belani, “Image Encryption using different techniques”, International Journal of Emerging Technology and Advanced Engineering ISSN: 2250-2459, Vol. 1,Issue1, Nov 2011.

[7] Nidhi Sethi, Ram Krishna, R. P. Arora, “Image Compression using HAAR Wavelet Transform”, IISTE Comp. Engg. & Intelligent Systems, ISSN 2222-1719, 2011

[8] Meenakshi Chaudhary, Anupma Dhamija, “A brief study of various wavelet families and compression techniques”, ,Journal of Global Research in Computer Science ISSN: 2229-371X, Vol. 4,Issue No. 4,April 2013.

[9] Q. M. Yao, W. J. Zeng, and W. Liu, “Multi-resolution based hybrid spatiotemporal compression of encrypted videos,” IEEE in Proc. ICASSP, Apr. 2009, pp. 725–728.

[10] D. Schonberg, S. C. Draper, C. Yeo, and K. Ramchandran, “Toward compression of encrypted images and video sequences”, IEEE Trans. Inf. Forensics Security, vol. 3, issue 4, Dec. 2008.

[11] Piotr Porwik, Agnieszka Lisowsk, “The Haar–Wavelet Transform in Digital Image Processing: Its Status and Achievements”, Machine Graphics and Vision, vol. 13, issue 1/2, 2004.

[12] Bryan Usevitch, “A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000”, IEEE Signal Processing Magazine, 2001.

[13] Haweel T.I., “A new square wave transform based on the DCT”, Signal Process., 2001.

[14] M. J. Weinberger, G. Seroussi, and G. Sapiro, “The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS”, IEEE Trans. Imag. Process., vol. 9, issue 8, Aug. 2000.

[15] X. Wu and N. Memon, “Context-based, adaptive, lossless image codec”, IEEE Trans. Commun., vol. 45, issue 4, Apr. 1997.

[16] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, Cleveland, OH, USA: CRC Press, 1997.

[17] Ch. Samson, V. U. K. Sastry, “An RGB Image Encryption Supported by Wavelet-based Lossless Compression”, International Journal of Advanced Computer Science and Applications, Vol. 3, Issue 9, 2012.

[18] Ambika Oad, Himanshu Yadav, Anurag Jain, “Image Encryption techniques and its terminologies”, International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014