International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Comparative Analysis on an Encrypted-Compressed Image using HAAR and COIFLET Wavelet Transform

Navita Palta[1], Neha Sharma[2]
[1]Deptt. of CSE, Chandigarh Engg. College,
Mohali, Punjab, India.
[1]*navitapalta@gmail.com*

[2]Associate Professor
Deptt. of CSE, Chandigarh Engg. College,
Mohali, Punjab, India.
[2]*er.nehasharma09@yahoo.com*

Abstract: Since multimedia data contains important as well as personal digital images and videos so, their storage, privacy and security are the most important issues while transmitting data openly over the network. In this work, firstly an image has been encrypted via prediction error clustering and random permutation. Then the encrypted image has been compressed using both HAAR and COIFLET wavelet using 2D level of decomposition. Finally, the results have been compared on the basis of different parameters: Compression Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Entropy, Bit Error Rate (BER) showing HAAR wavelet is better than COIFLET wavelet.

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

I. INTRODUCTION

The privacy of multimedia is very important because multimedia data are transmitted openly over the networks more frequently[10]. Therefore, reliable security is needed for content protection of digital images and videos. Encryption schemes for multimedia data secure the multimedia content and fulfill the privacy requirements for a particular multimedia application. Encryption is a process of changing the image format into unreadable format so that it cannot be read by intruder.

Larger progresses are made in the field of image compression. Image compression is deals with removing redundant information of image data and it provide a way of solution associated with storage and data transmission problem of huge amounts of data for digital image[18]. Application of Imag 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 reduces the cost associated with sending the data over network.
- It helps in reducing storage requirements.
- It handles the probability of transmission errors as less bits are transferred.
- It provide privacy against illegal monitoring.

The above mentioned benefits and requirements of image encryption and image compression. Therefore, 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 scenario in which a data owner Alice wants to securely and efficiently transmit an image to the Bob who is the receiver of the system.

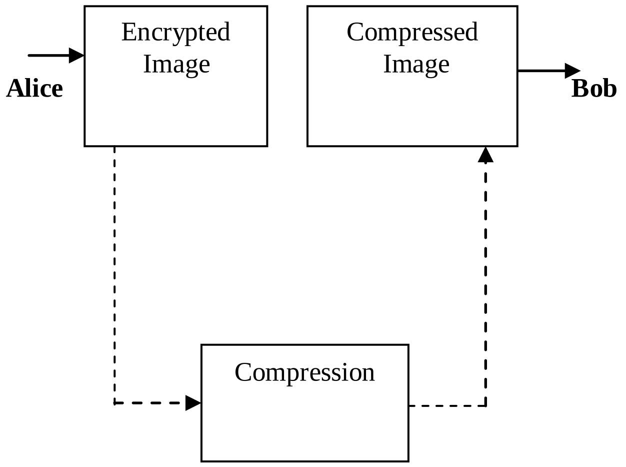

Figure 1: Encryption and Compression System

In the above Figure 1 Encryption-Compression Scheme is presented, in this image is first encrypted using prediction error clustering and random permutation methods as encryption technique and then the encrypted image is compressed using HAAR and COIFLET wavelet transform.

II. TECHNIQUES USED

There are two main techniques that are used for compression. These techniques are explained below:-

2.1. HAAR Wavelet

The HAAR wavelet is also the simplest wavelet. The Haar wavelet is a simple form of compression which involves storing detail coefficients, eliminating data, and reconstructs the matrix so that the resulting matrix is similar to the initial matrix. It represents the similar wavelet as Daubechies db1. Hungarian mathematician Alfred Haar invented this wavelet.

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

$$\psi(t) = \begin{cases} 1 \\ -1 \\ 0 \end{cases}$$
$$0 \le t < \frac{1}{2},$$
$$1/2 \le t < 1, \text{ otherwise}$$

Scaling function φ (t) can be described as:

$$\phi(t) = \begin{cases} 1 \\ 0 \end{cases}$$
$$0 \le t < 1, \text{ otherwise}$$

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.
- It can be used to analyse the localized feature of signals which include frequency, amplitude of the signal.

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 The wavelets are symmetric in nature because if function as are computed from left hand side results are same if they are computed from right hand side and its function have scaling functions N/3-1 which are used in different applications . 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: Original image is taken

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 separately with encryption algorithm are applied on the input image.

Phase 5: Compare results with each other.

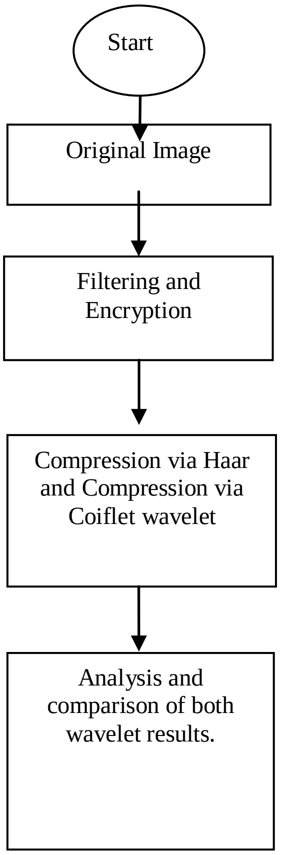
Start
Original Image
Filtering and Encryption
Compression via Haar and Compression via Coiflet wavelet
Analysis and comparison of both wavelet results.

Figure 2. Flow Chart of Proposed System

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.

$$C_R = n1/n2$$

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 tables are showing the comparative analysis of HAAR and COIFLET wavelets on the set of 10 images and there average is also evaluated whereas the bar graphs shows the comparison between 5 images.

Table 1: Comparison of Lossy compression performance using HAAR wavelet

IMAGES	MSE	PSNR	ENTROPY	BER	CR
Airplane	2.86	50.1	6.70	2.26	1.64
Baboon	2.84	48.0	7.45	4.21	1.64
Mona Lisa	2.97	48.3	7.57	4.13	2.04
House	2.84	48.0	6.46	4.29	1.64
Snap	2.85	48.2	7.30	4.10	1.64
Dog	2.84	48.1	7.80	4.20	1.64
Baby	2.91	48.8	7.38	4.12	1.64
Man	2.84	50.2	7.49	3.19	1.64
Boat	2.83	50.3	6.94	3.21	1.23
Lena	2.86	50.1	7.52	3.21	1.64
Average	2.86	49.0	7.26	3.69	1.63

Table 2: Comparison of Lossy compression performance using COIFLET wavelet

IMAGES	MSE	PSNR	ENTROPY	BER	CR
Airplane	2.96	49.9	6.08	2.27	1.64
Baboon	2.94	47.8	7.02	4.22	1.64
Mona Lisa	3.07	48.1	7.50	4.14	2.04
House	2.94	47.8	6.46	4.30	1.63
Snap	2.95	48.0	7.20	4.11	1.64
Dog	2.93	47.9	7.72	4.21	1.64
Baby	3.00	48.6	6.73	4.13	1.64
Man	2.94	50.0	6.75	3.20	1.64
Boat	2.93	50.1	6.81	3.22	1.23
Lena	2.96	49.9	7.40	3.22	1.63
Average	2.96	48.8	6.96	3.70	1.63

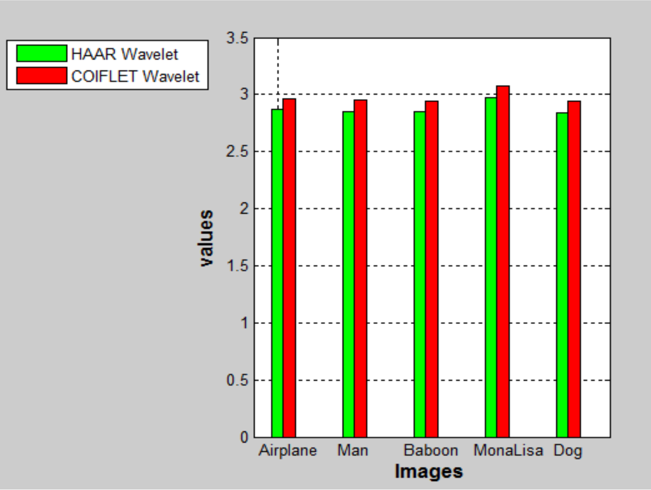

Fig 3: Graph showing comparison of MSE values between HAAR and COIFLET wavelet.

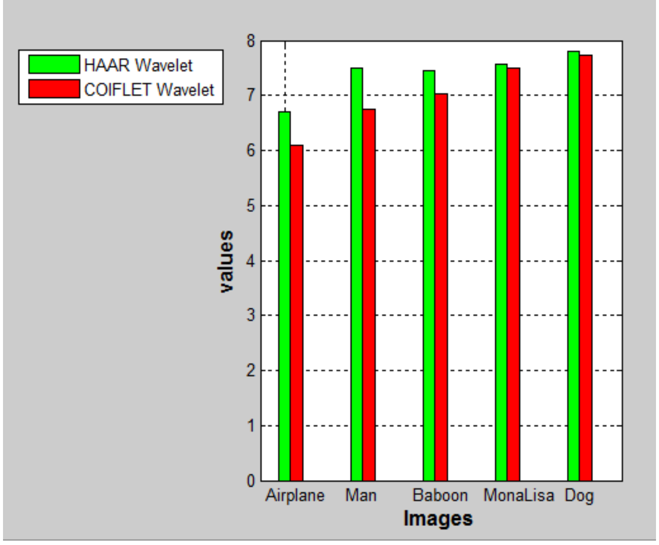

Fig 4: Graph showing comparison of ENTROPY values between HAAR and COIFLET wavelet.

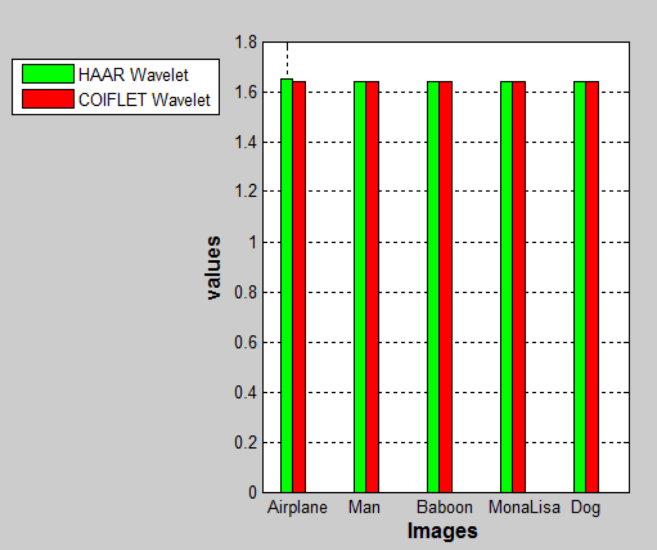

Fig 5: Graph showing comparison of CR values between HAAR and COIFLET wavelet.

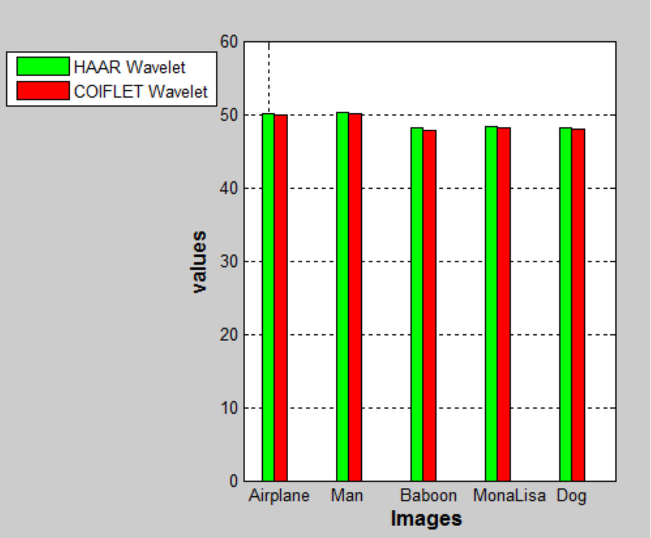

Fig 6: Graph showing comparison of PSNR values between HAAR and COIFLET wavelet.

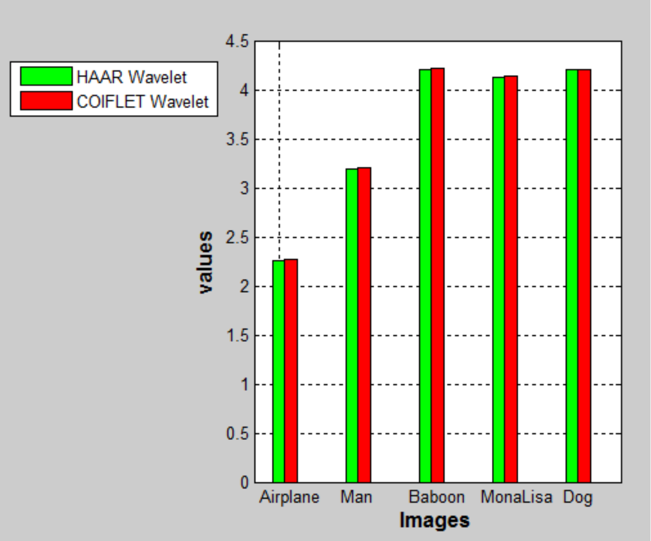

Fig 7: Graph showing comparison of BER values between HAAR and COIFLET wavelet.

From above bar graphs it is clear that HAAR wavelet is better than COIFLET wavelet because MSE, BER is less in case oh HAAR in comparison to COIFLET wavelet. PSNR, ENTROPY and CR values are greater in case of HAAR wavelet than COIFLET wavelet. So, it is observed that HAAR wavelet provide better results than COIFLET wavelet.

VI. CONCLUSION AND FUTURE SCOPE

This research work designs an efficient image for Encryption and Compression system. In this work image encryption is done by prediction error clustering and random permutation methods. Highly efficient compression of encrypted image realized by a new image compression algorithm of Haar and COIFLET wavelet transform. The Experimental results shows that when 2D level of decomposition is done on an encrypted image via HAAR and COIFLET wavelet, HAAR wavelet results are better than COIFLET as all the parameters value are higher in case of HAAR therefore, indicates the obtained image are of higher quality in case of HAAR. 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 loss-less 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