Designing an Efficient Image Encryption-Compression System using a New HAAR, SYMLET and COIFLET Wavelet Transform

Sukhpreet Kaur
Indo Global Group of Colleges

Vanita Rani
Assistant professor
Indo Global Group of Colleges

ABSTRACT
In the modern world, hidden information plays a decisive role in protecting the data and reducing the space in the memory as well as on disk drives. If encryption and compression works properly than it leads to high speed computation. Encryption of an image can be done in many ways and several techniques use different methods for encryption. Image encryption scheme operated in the prediction error domains which are able to provide a high level of security reasonably, after that we can efficiently compress the encrypted images. In this paper the full image is encrypted in an efficient and secure manner with Data Encryption Algorithm along with a new modified International Haar, SYMLET and COIFLET Wavelet. After achieving encryption on the original file, compression will be performed to obtain a compressed image. The approach based on Arithmetic coding is also demonstrated which can be utilized efficiently to compress the encrypted images. The existing encryption-then-compression (ETC) solutions encourage significant forfeiture on the compression efficiency. For better compression efficiency we are using HAAR and COIFLET wavelet transform along with ETC, for the implementation of this proposed work, the Image Processing Toolbox under MATLAB software is used.

Keywords
encryption, compression, ETC, Haar wavelet, wavelet and Coiflet wavelet.

1. INTRODUCTION
Encryption is the most persuasive way to enact data security. It is the process in which information is encoded in such a way that only authorized recipient can decode it. In this, information is changed to make it meaningless for everyone but except for those who obtain special knowledge which authorize them to change information back to its original form. Encryption is important because it consent us to secure and protect the data. This is used to protect the secrets of corporate as well as government's offices. Mainly used to secure the classified information, where as many individuals use encryption to protect their personal information so as to defend themselves against situations like identity theft, cyber crime, etc. There are two types of encryption; they are symmetric encryption and asymmetric encryption. In symmetric encryption, the encryption and decryption keys are the same where as in case of asymmetric encryption there are different keys used for both encryption and decryption. The advantages of encryptions are as follows.

Contentment or Peace of Mind

Protection from Identity Theft

Protection from Unauthorized Access

Safe Decommissioning of Computer

Agreement with Data Protection Acts

Compression: It done in order to save space or transmission time. The meaning of compression is reduction in size. The main objective behind compressing an image is to minimize the irrelevant and redundant data, so as to store or transmit data in more efficient way. The applications of data compression are as follows

- Hard Disk Compression
- Distributing Software
- Data Transmission

Image compression can be lossless or lossy. Lossless compression is preferred for archival purpose, medical imaging, technical drawings where as lossy compression methods are used at low bit rates, especially for natural images such as photographs. With the rapid development in the field of multimedia and network technologies, the security of multimedia becomes more and more crucial. The multimedia data are transmitted over open networks more and more frequently, where the security is reliable and necessary to provide protection to the content of digital images and videos. For a specific multimedia application, the encryption for multimedia data needs to be specifically designed to ensure that the media content is interactive and satisfy the necessities related to security.

Government agencies, private businesses and military accumulate great deal of secret and confidential images about their patient in hospitals, land ranges in expedition, antagonist positions in safeguard, item and monetary status. All this data is collected and insert on electronic PCs and then transmitted over across the system to other PC. If the confidential images regarding the antagonist positions, persistent and geological zones decline into the wrong hands, than such a breach in security could prompt piles of war and wrong treatment. This information is stored in the computer system in the form of files because files are considered as basic entity for keeping the information.

Good encryption makes a source look completely random and traditional algorithms are not able to compress encrypted data. The traditional systems make a point to compress before encryption. We are using the concept of public key encryption for the purpose of encryption and decryption of image. In this system, a public key of sender and receiver is known to both, but private keys are kept secret. This is done so that neither the compression efficiency nor the security will be sacrificed by performing compression in the encrypted realm. After encryption and compression, reconstruction of original image takes place.

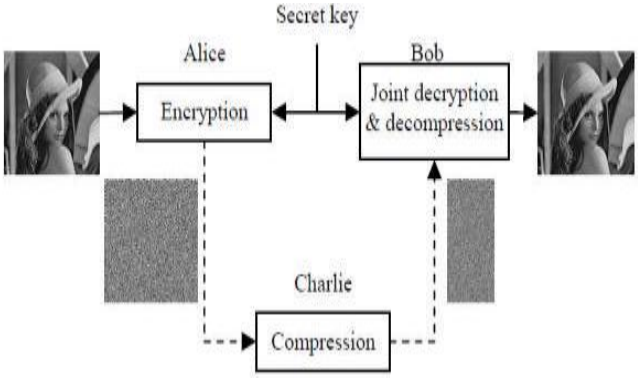


Fig1: encryption then compression system

Consider an application scheme in which a substance owner Alice needs to safely and productively transmit an image I to a recipient Bob by means of an un-trusted channel provider Charlie. This should be possible as, Alice first packs I into B and after that rush B into Ie utilizing an encryption capacity EK (•) where K denotes the secret key and the encoded information Ie is then gone to Charlie and simply forwards it to Bob and receiving Ie Bob sequentially performs decryption and decompression to get a reconstructed image I.

The Compression then Encryption (CTE) standard meets the prerequisites in numerous protected transmission structures the request of applying the pressure and encryption needs to be switched in some other condition. Alice is always interested in security the solitude of the image data over encryption. Alice has no motive to compress her information and consequently won't utilize her constrained computational assets to run a pressure calculation before encryption of information. This is mystery key genuine when Alice utilizes an asset example cell phone. In this contrast the channel provider Charlie has a highest enthusiasm for packing all the system activity in order to boost the system usage. It is tremendously coveted if the pressure undertaking can be assigned by Charlie and who regularly has bounteous computational assets.

A major test inside such Encryption then Compression structure is that pressure must be controlled in the encoded space as Charlie does not access to the mystery key K and this sort of ETC framework is indicate in Figure. The likelihood of preparing encoded flags specifically in the scrambled area has been getting expanding perception as of late. At the first peep it is by all accounts outlandish for Charlie to pack the scrambled information since no sign structure can be use empower an old compressor.

Albeit illogical and Johnson demonstrated that the stream figure encoded information is compressible through the utilization of coding with side data standards without trading off either the pressure proficiency or the data theoretic security. By applying LDPC codes in different bit-planes and abusing entomb and intra relationship, Lazzeretti and Barni exhibited are a few routines for lossless pressure of scrambled Gray Scale shading pictures. Notwithstanding the hypothetical discoveries additionally proposed down to earth calculations to misfortune lessly pack the scrambled parallel pictures. Schonberg later researched the issue of packing encoded pictures when the fundamental source measurements are obscure and the sources have memory.

2. WAVELET

A mathematical function which cut up data into different frequency components, and then study each component with a resolution matched to its scale is known as Wavelet. In analyzing physical situations where the signal contains

discontinuities and sharp spikes, wavelet method has many advantages over the traditional Fourier methods. These are the functions which satisfy certain mathematical requirements and are used in representing data or other functions. This idea is not new; since the early 1800's, approximation using superposition of functions has existed when Joseph Fourier discovered that he could superpose sines and cosines to represent other functions. However, in wavelet analysis, the scale that we use to look at data plays a special role. At a determination interpreted information can then be sorted which matches its scale. The procedure of wavelet analysis is to adopt a wavelet prototype function, known as an analyzing wavelet or mother wavelet. There are two types of analysis i.e. temporal analysis and frequency analysis. Temporal analysis is performed with a contracted, high-frequency version of the prototype wavelet, where as frequency analysis is performed with a dilated, low-frequency version of the same wavelet.

2.1 Coiflet Wavelet

Coiflet wavelets are discrete wavelet outlined by Ingrid Daubechies, on the requisition of Ronald Coifman, to have scaling operations with vanishing time period. The wavelet is closing symmetric and their wavelet operation has N/3 vanishing time period and the scaling operation is N/3-1. They have been utilized in numerous applications by the use of Calderón-Zygmund Operators. Both the scaling operation and the wavelet operation must be normalized by a consideration $1/\sqrt{2}$. The following are the coefficients for the scaling operations for C6-30. The wavelet coefficients are demonstrate by switching the request of the scaling capacity coefficients and after that turning around the indication of each second one (i.e. C6 wavelet = {−0.022140543057, 0.102859456942, 0.544281086116, −1.205718913884, 0.477859456942, 0.102859456942}).

Scientifically, where k is the coefficient file and B is a wavelet coefficient and C a scaling capacity coefficient and N is the wavelet record i

Fig4: Coiflet with two vanishing moments

2.2 Haar Wavelet

In mathematics Haar wavelet is a sure grouping of capacities. It is perceived as the first known wavelet and this succession was proposed in 1909 by Alfred Haar. Hence this wavelet is named after Alfred Haar. The Haar wavelet is additionally the most straightforward conceivable wavelet. There is a disadvantage of the Haar wavelet and that is it is not ceaseless and not differentiable. It utilized the capacities to give sample of calculable ortho ordinary framework for the space of square

integrals works on the genuine line. The investigation of wavelets even the term wavelet did not come until much later.

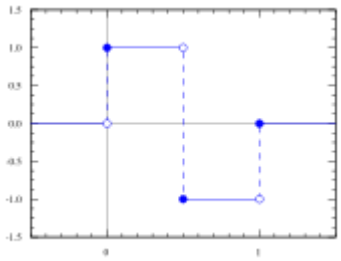


Fig 2 : haar wavelet

The Haar wavelet's mother wavelet function is ψ (*t*) can be described as

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

And its scaling function φ (*t*) can be trace as

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

The Haar wavelet works on information by determining the totals and contrasts of adjoining components. It can be works on both i.e. first on neighbouring even components and afterward on adjoining vertical components. The Haar change is utilizing:

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

2.3 SYMLET WAVELET

Symlet wavelets are the adjusted adaptation of Daubechies wavelets with expanded symmetry. They are likewise measurements and minimalistically upheld wavelets, which are proposed by I. Daubechies. Symlet are closely symmetric and have the slightest asymmetry. The scaling filters used are close direct stage filters and the impact of Symlet is almost same as those of the Daubechies wavelets. The Symlet wavelet and scaling operation for requests are as shown below:

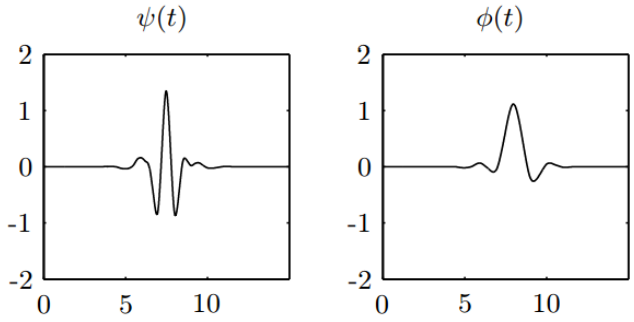


Fig 3: symlet wavelet function and scaling functions

The Symlet wavelets are also known as Daubechies' slightest lopsided wavelets but they are more symmetric. In Symlet wavelet, N is the quantity of variable time period. These kind of channels are additionally advert to in the writing by the quantity of channel taps and which is 2N. In MATLAB enter wave data ('sym') in order to obtain an overview of the fundamental properties.

2.4 ETC SYSTEM

The scheme includes the details of the three key components in modified ETC system, first is image encryption control by Alice, and second is image compression control by Charlie and then bob controlled the logical order decryption and decompression. Encryption is the process in which plain text is converted into unreadable form to provide the high level of security. To decrypt or decode the text, the receiver use that key which is used for encrypting the text [7]. Encryption method is used of securing the data which is very important and confidential for the military and the government operations. Now a day it is also used by the civilian's in day-to-day life. There are various applications like in the online transactions of banks and the data transfer via networks and exchange of vital personal information etc. All these require the application of encryption from the aspects of reliability and security. The work which is done earlier only addressed the compression of bi-level images and binary i.e. black and white images with asymmetric probabilities of black and white pixels. The growth of lossless compression of the encrypted images has been recently signified by relying on the comparison with source coding and the side information at the decoder. Bob aims to retrieve the original l image I after receiving the compressed and encrypted bit stream B. A multimedia technology used for hiding information which provides the authentication and copyright protection.

3. ARITHMETIC CODING

It is most often used when we have to code binary symbols or bits. Each bit begins the coding process. The arithmetic codes generate non-block codes; that is a correspondence between source symbols and code words does not exist. Instead, an entire sequence of source bits is allocated to a single code word which defines an interval of real numbers between 0 and 1.

As the number of symbols or bits in the message increases, the interval used to represent it becomes smaller and the number of bits needed to represent the interval becomes larger. Each symbol in the message reduces the size of the interval according to its probability of occurrence. Since the symbols are not coded one at a time, this technique can achieve the highest possible coding efficiency.

4. METHODOLOGY

The methodology of performing the image encryption-compression by new Haar and Daubechies wavelet transform includes following steps:

Step 1: Implementation of encryption algorithm to the input image I.

I: Compute all the mapped prediction errors $\tilde{e}$i, j of the whole image I using GAP image predictor.

II: Divide all the prediction errors into L clusters Ck, for $0 \le k \le L - 1$, and each Ck is formed by concatenating the mapped prediction errors in a raster-scan order.

III: Reshape the prediction errors in each Ck into a 2-D block having four columns and $\lceil |C_k|/4 \rceil$ rows, where |Ck| denotes the number of prediction errors in Ck.

IV: Perform cyclical shift operations to each resulting prediction error block, and read out the data in raster-scan order to obtain the permuted cluster $\tilde{C}$k.

V: The assembler concatenates all the permuted clusters $\tilde{C}$k, for 0 ≤ k ≤ L− 1, and generates the final encrypted image Ie=$\tilde{C}0\tilde{C}1\ldots\tilde{C}$L-1, in which each prediction error is represented by 8 bits. As the number of prediction errors equals that of the pixels, the file size before and after the encryption preserves.

VI: Pass Ie together with the length of each cluster |$\tilde{C}$k |, for 0≤k≤L− 2.

Step 2: Implementation of compression algorithm to the outcome of above algorithm i.e. Ie.

I. Treat the array as n/2 pairs called (a, b)

II. Calculate (a + b) / sqrt(2) for each pair, these values will be the first half of the output array.

III. Calculate (a - b) / sqrt(2) for each pair, these values will be the second half.

IV. Repeat the process on the first half of the array (the array length should be a power of two).

V. The proposed sparse orthogonal transform matrix can be obtained by appropriately inserting some 0's and ½'s into the HWT.

VI. It is look at the first four entries of as two pairs that it will take their averages. The third and the fourth entries are obtained by subtracting these averages from the first element of each pair.

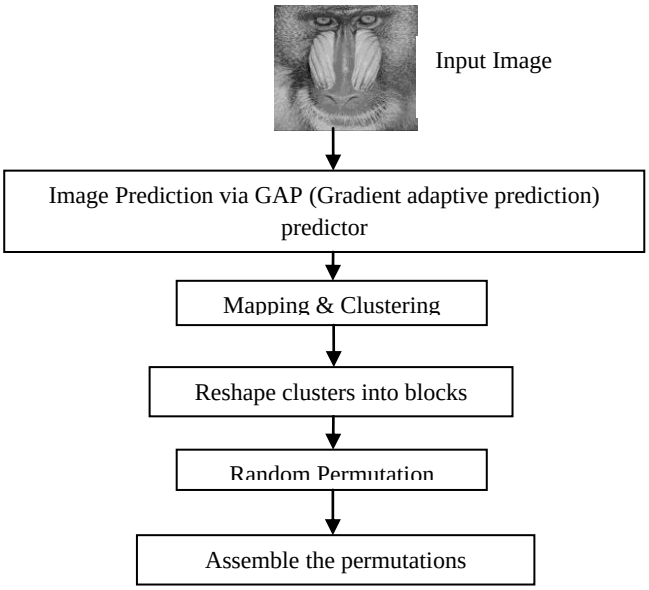
VII. Average the first two entries and before subtract the answer from the first entry.

Step 3: Applying the reverse process for decompression & decryption.

I: Calculate the inverse of all the intermediate matrices and multiply them.

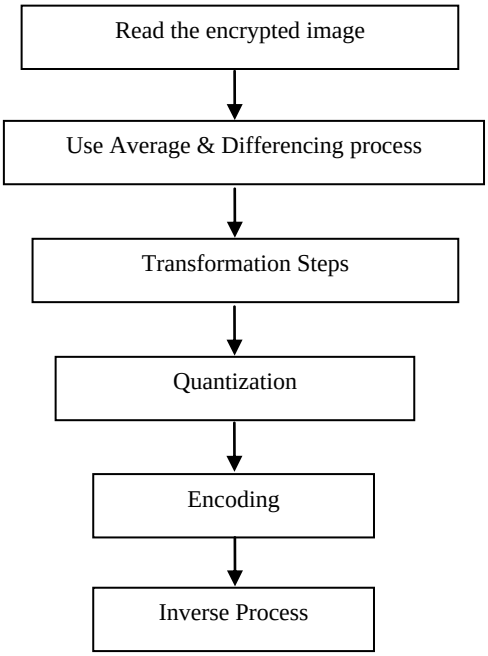
II: Real image will retrieved by the resultant matrix.

Step 4: Calculate the CR, MSE & PSNR of the reconstructed image.



All these steps, from input image to the assembling of the permutation are involved in Encryption of an image.

The steps shown below are used for compression of the encrypted image. These steps utilize new algorithm of HWT, Daubechies.



In this new image compression algorithm of Haar and Daubechies wavelet transform, the main difference from the old algorithm is that in the previous one each row and column was gone through sum and differencing but in the new one each row and column go through average and differencing.

5. EXPERIMENTAL RESULTS

In this section, we perform experiments to verify the efficacy of our approach. The comparison of the accuracy is done for every method is one with the given values to the proposed work. The accuracy rate is much higher in the proposed work as compare to the previous working methods.

6. 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-

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

PSNR is 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.

V.II Average Rate 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.

In the fig 5 and fig 6 shown below, shows the bar graph of average rate and average PSNR calculated.

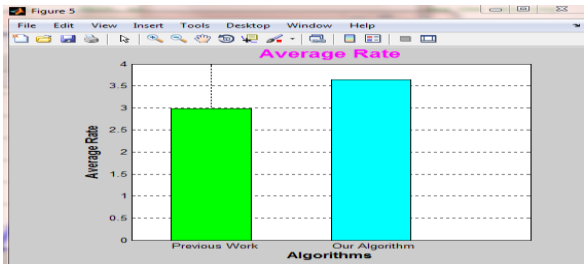


Fig 5. Average Rate Comparison

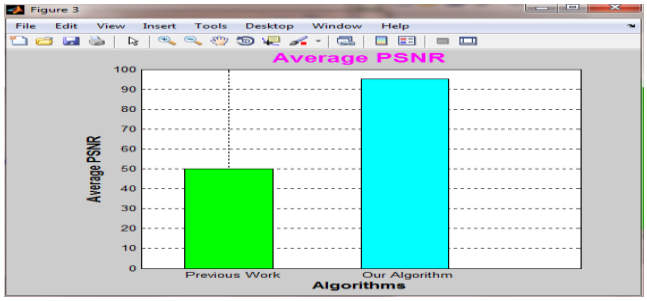


Fig 6. Average PSNR Comparison

The graph in fig 7 shows the PSNR graph obtained using ETC along with HAAR and COIFLET.

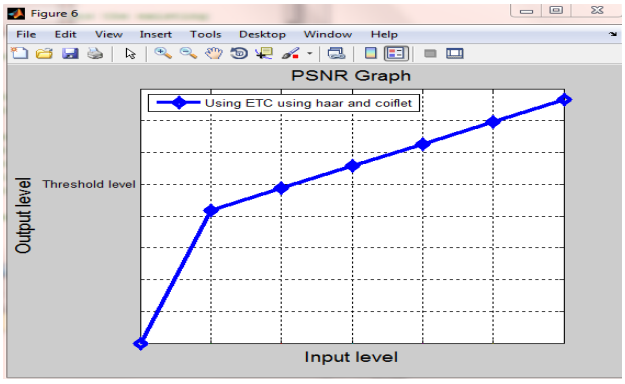


Fig 7. PSNR graph

All the graphs show the comparison between the previous approach and the proposed approach. This is

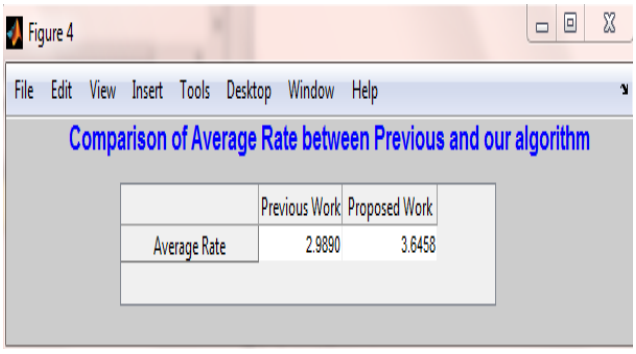


Fig 8. Comparison of Avg Rate between Previous and our algorithm

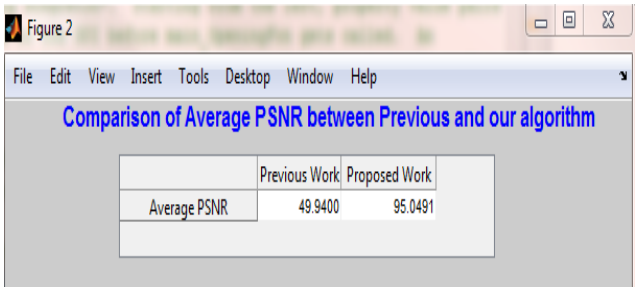


Fig 9. Comparison of Avg PSNR between Previous and our algorithm

In fig 8 and in fig 9 the comparison is shown between the previous and our algorithm. The average rate obtained by proposed approach is approx 3.6 and the average PSNR is approx 95, which high as compared with the previous work.

7. CONCLUSION

In this paper we have designed an efficient image Encryption-Compression system using HAAR wavelet and COIFLET wavelet. In the proposed scheme, the encryption of image has been obtained by random permutation. An efficient compression of encrypted image has been accomplished by using a new image compression algorithm based on Haar and Coiflet wavelet transform. Experimental results show that our algorithm has high level of security as compared with the previous algorithms. For resultant images the PSNR values are better than the previous one. Better PSNR specify that the reconstruction of image is of higher quality. The coding efficiency of our proposed compression method on encrypted images is very close to that of state of art loss image codes which receive original and unencrypted images as input. This shows that our encryption-compression system is more efficient.

8. FUTURE SCOPE

This paper is limited to compression of single image .We can extend our research to work on the different images simultaneously .Also in future more parameters like by enhancing the number of pixels quality can be considered. As we can also extend this work for the infinite number of users. Wean further apply new formulas or algorithm for the enhancement of compression ratio in compressing of images and reducing time for execution. The proposed algorithm can be implemented on different tools also.

9. REFERENCES

[1] Jiantao Zhou, Xianming Liu, Oscar C. Au and Yaun Yan Tang, "Designing an Efficient Image Encryption Then Compression System via Prediction Error Clustering and Random Permutation", IEEE Transactions on Information Forensics & Security, Vol. 9, Issue.1, January 2014.

[2] Lisa M. Marvel and George W. Hart wig, Jr. ,"A Survey of Image Compression Techniques and Their Performance in Noisy Environments", IEEE Transactions on Circuits & Systems for Video Technology, Vol. 23, Issue.2, pp.311-325, IEEE 2013.

[3] Jashanbir Singh Kalka, Reecha Sharma, "Comparative Performance Analysis of Haar, Symlet and Bior wavelets on Image compression using Discrete Wavelet Transform", International Journal of Computers & Distributed System, Volume 1, Issue 2, August, 2012.

[4] 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.

[5] Kamrul Hasan Talukder and Koichi Harada, "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", IAENG International Journal of Applied Mathematics, 36:1, IJAM_36_1_ Dec 2012.

[6] M. Sifuzzaman1, M.R. Islam and M.Z. Ali, "Application of Wavelet Transform and its Advantages Compared to Fourier Transform." Journal of Physical Sciences, Vol. 13, 2009.

[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2009

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

[9] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.

[10] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[11] R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey- level and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.

[12] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.

[13] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted GrayScale images," IEEE Trans. Image. Process. vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[14] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Image. Process. vol. 21, no. 6, pp. 3108–3114, Jun. 2012.

[15] R. Mehala and K. Kuppusamy, "A New Image Compression Algorithm using Haar Wavelet Transformation", International Journal of Computer Applications, International Conference on Computing and Information Technology, 2013.

[16] X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multilayer decomposition", Multimed. Tools Appl., vol. 78, issue 3, Feb. 2013.

[17] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing", IEEE Trans. Inf. Forensics Security, vol. 7, issue 3, June 2012.

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

[19] V. Ashok, T. Balakumaran, C. Gowrishankar, Dr. ILA.Vennila, Dr.A.Nirmal kumar, "The Fast Haar Wavelet Transform for Signal & Image Processing", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, issue 1, 2010.

[20] 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.

[21] 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.

[22] U. Maurer, "The strong secret key rate of discrete random triples," in Communication and Cryptography—Two Sides of One Tapestry, R. Blahut, Ed. Norwell, MA: Kluwer, 1994, pp. 271–285.

[23] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in Advances in Cryptology—EUROCRYPT, vol. 1807, Springer-Verlag Lecture Notes in Computer Science, B. Preneel, Ed., 2000, pp. 351–368.