HYBRID COMPRESSION TECHNIQUE USING ENCRYPTION AND DAUBECHIES WAVELET

Sunil Khullar,[1]Er. NandiniChauhan[2]
[1]Assistant Prof., [2]Research Scholar
[1,2]Department of Computer Science and Engineering, Rayat Institute of Engineering and Information Technology College, Railmajra, SBS Nagar, (Punjab) India
[1]sunilkhullar222@yahoo.co.in, [2]nandini330@gmail.com

***ABSTRACT*:- The rapid development is a crucial resolution problem in the multimedia and network technologies where the privacies and securities become the important issues in the multimedia which transmitted openly over the network. The storage space is atraditional era that can't be missed. That's why to improve the privacy as well as security to the multimedia, encryption work through the root for encrypted input image as well as the decrypted for output image in compression and decompression and similarly for reduction the storage space by compression. Reduction in size will also decreases the time which taken for transmission over multimedia technologies. Therefore, many practical scenarios where image encryption including the conducted prior to image compression. This causes how to design the problem with a pair of image encryption as well as compression algorithms which compresses encrypted images to be efficiently performed. In this work, we have done design and implementation of an image with encryption-compression system, where considering the matrices psnr, mse, entropy, and ber. The proposed scheme works on image encryption with random permutation method which provides reasonably high level of security with high level of resolution. Here, also implementing a new image compression algorithm where using the Daubechies Wavelet Transform that may be used efficiently compresses the encrypted image. The quality of the image at the receiver side are guaranteed and more notably approach applied for compression to encrypted image that considered more efficient for entropy, Mean Square Error, and Peak Signal to Noise Ratio, and ber.**

***KEYWORDS:*-Median filter, Encryption-Then-Compression, Daubechies Wavelet**

I. INTRODUCTION

The multimedia security becomes more important, where the multimedia data are transmitted over the open networks more frequently. Typically, it is reliable for security which is necessary to contentprotection of digital images and videos. The multimedia Encryption schemeneeds to be specifically designed for the protection of multimedia content and fulfil the security requirements in a particular multimedia application. For example, for an image real-time encryption using classical ciphers which requires heavy computation due to the large amounts of data used, but many applications of multimedia requires security on a lower level, that can be achieved by using encryption selectively that leaves some perceptual information after encryption. Government, military and private business amass great deal of confidential images related to patient in Hospitals, geographical areas in research, enemy positions in defenceof product and financial-status. This information collects and stored on electronic computers to transmit across network to other computer. Therefore, ifthese confidential images about the patient, an enemy position over geographical areas fall into the wrong person than such a breach of security could lead to lots of war and wrong treatment etc. Protecting confidential images is the legal and an ethical requirement. It stores information in the form of filesin computer system. File is considered as a basic entity for keeping the information. After that the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is worldwide accepted fact that securing file data is very important, in today's computing environment. Good encryption makes a source lookrandomly; traditional algorithms are not successful to compress encrypted data. For this reason, traditional systems make sure to compress before they encrypt. We are using the concept of public key encryption, for the encryption and decryption of image. In this public key's of sender and receiver is known to both but private key's are kept secret. The securityand the compression efficiency will not be sacrifice by performing compression in the encrypted domain. In addition, thetheoretical findings help proposed practical algorithms to losslesscompression the encrypted binary images. Schonberg later found the problem of compressing encrypted images to underlying source statistics that was unknown and the sources have memory. By applying LDPC codes in different types of bit-planes and exploiting to inter/intra correlation value, Lazzeretti and Barn presented several separate methods for lossless compression encrypted GrayScale/color images.

II. LITERATURE SURVEY

Jiantao Zhou et al. (2014) designed a highly secure toefficient image encryption-then-compression (ETC) system,

where both methods, lossless and lossy compressions are taken. Therefore proposed figure encryption scheme for prediction error domain. They showed to be able to provide more reasonably high level of security. Here it is shown that an arithmetic coding-based technique can be expressedand compressed the encrypted imagessuccessfully. Then proposed compression approach was applied to encrypted images. It is only slightly worse to compression efficiency for the state-of-the-art lossless/lossyimage coders andtakes original and unencrypted images as inputs. Both theoretical and experimental results have shown that more reasonably high level of security has been retained.**S. ParveenBhanu et al. (2011)** presented a novel hybrid image compression technique for suitable storage and delivery of data. This depends on decomposing the data through daubechies-4 wavelet in combination - lifting scheme and entropy encoding. Therefore this technique is focused onmetrices compression ratio, bits per pixel and peak-signal-to-noise-ratio on basis of experimental results illustrate that the proposed.**ManikGroach et al. (2012)** presented an efficient hybrid image compression method and helped combining the features of two separate techniques as such - DCT and SPIHT. First the image is compressed using DCT to low frequency component to compress. In order, the compressed image has decomposed using bi orthogonal wavelet transform. The decomposed output further compressed by SPIHT encoding to achieve high frequency component in compression. The reconstruction of the original image involved the linear combination for corresponding processes as take in image encoding. The reconstructed image is use for quality achievethrough decoding inprocess to desirable quality. Experimental results haveshown that the DCSPIHT gave better close quality to the SPIHT.**SandeepKaur et al. (2013)** evaluated a set of wavelets for image compression and figure compression using wavelet transforms results to improved compression ratio. Therefore, Wavelet transformation technique provides both spatial and frequency domain information for comparative analysis of Haar and Coiflet wavelets in form of metrics PSNR, Compression Ratio and Elapsed time in compression using discrete wavelet transform. Discrete wavelet transform has important role over Fourier transform based techniques. DWT removes the problem of blocking that occurs in DCT. DWT provides better image quality than DCT to attain higher compression ratio.**SherinKishk et al. (2011)** proposed principle component analysis technique to apply on the wavelet coefficients of the elemental images to optimize the quality of the recovered 3D image to achieve high compression ratio. Then wavelet coefficients of the each elemental allowed to stacked and rearranged before applying PCA compression. Then PCA compression is applied to every sub-band to enhance the compression ratio individually. Therefore, quality of the reconstructed 3D images received elemental images to calculate. And results have shown great compression ratio compared to PCA alone compression in maintaining the recovered 3D image quality. At last,PSNR measured the reconstructed 3D image quality for further used.

PROPOSED METHOD

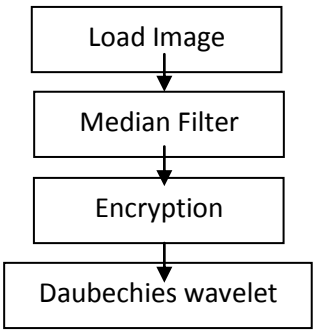


Figure 1 – Proposed Model of Compression and Decompression

III. DAUBECHIES WAVELET TRANSFORM

The Daubechies wavelets is based on the work of Ingrid Daubechies, are a member of family of orthogonal wavelets that defines a discrete wavelet transform and characterized by maximum number of vanishing moments has been given to support in compression. Every type of wavelet of this class, there is a scaling function (known as the father wavelet) which generates an orthogonal Multi-resolution analysis. In general, the Daubechies wavelets are so chosen such as to have the large number of vanishing moments, (this does not mean the best smoothness) for given support width N=2A. There exist two naming schemes that are in use, DN uses the length or number of taps, and dbA stands for the number of vanishing moments. So that D4 and db2 are the same wavelet transformsequently. It gives among the 2^{A-1} possible solutions based on algebraic equations for the moment inorthogonality conditions, one of them is chosen using scaling filter for extreme phase so that the wavelet transform is simple in practice using the fast wavelet transform. Daubechies wavelets are used in solving a wide range of problems such as to findin self-similarity properties of a signal or fractal problems, signal discontinuities, etc.

The Daubechies wavelets never defined for scaling and wavelet functions in large era; in fact, it is impossible to write down in closed form. Graph generated using the cascade algorithm using a numeric technique consists simply inverse-transforming [1 0 0 0 ...] many times. Daubechies orthogonal wavelets D2-D20 respectively and db1-db10 is commonly used for index number. The index number refers to the number N of coefficients for each wavelet, this index consists a number of zero moments or vanishing moments equal to half the number of coefficients to measure.

Prediction Error Clustering and random permutation

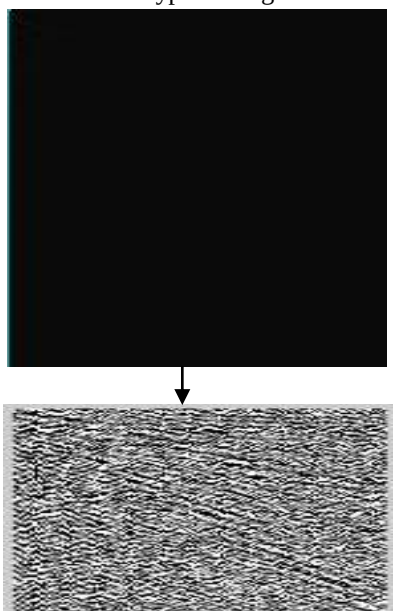
The prediction error clustering and random permutation algorithm works for encryption for transmit the input image. It is much related to state of the art loss less/lossy image codec to transmit the input image.

Process:

Original Image

Median Filter

Encrypted image



Decrypted Image

Figure 2, Comparison of previous and proposed algorithm

IV. RESULT AND DISCUSSION

In the figure 1, we have evaluated the bit error rate, entropy, mse, and psnr. These matrices are compared to the previous work and the proposed method. The Daubechies wavelet works better on the basis of above matrices as compared to the previous methods.

Comparison of between Previous and our algorithm

	Previous Work	Proposed Work
BER	2.3020	1.3516
ENTROPY	6.6975	7.0960
MSE	1.9890	1.6510
PSNR	49.9100	52.5567

Table 1, Comparison of previous and proposed algorithm

PSNR - In figure 1, peak signal to noise ratio has been calculated to previous method and proposed method from encrypted form to decrypted form to measure the image strength. This shows the clarity of image to receive by receiver. It should be high.

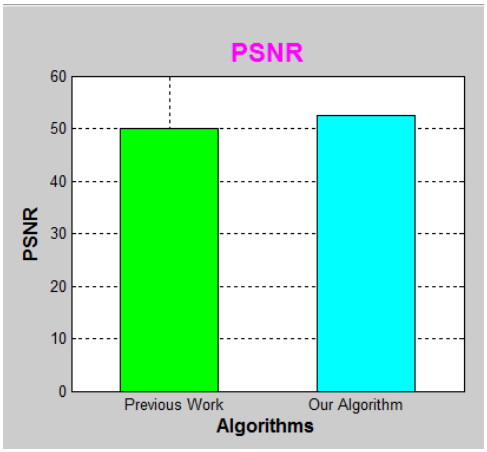


Figure 3, Comparison of psnr

MSE - In figure 2, mean square error is calculated for the previous work and the proposed work. It is also used for strength of image to encrypt sender side to decrypt image on receiver side. It should be minimized at the receiver side at the time of receiving decrypted image.

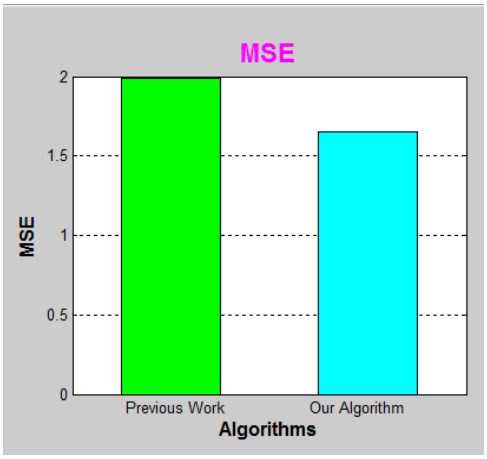


Figure 4, Comparison of mse

Entropy - In figure 3, the entropy is compared for the previous method and proposed method. The entropy should be same for encrypted image and decrypted image. The entropy is better of our method as compared to the previous method.

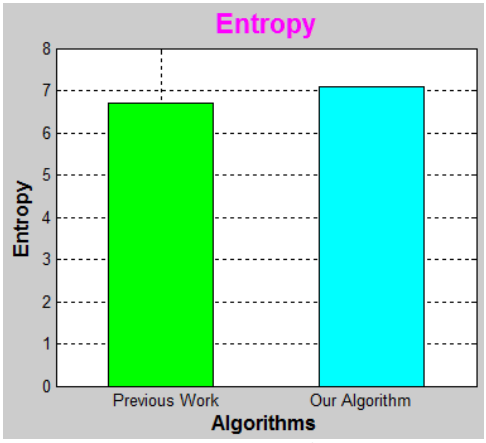


Figure 5, Comparison of entropy

BER - In figure 4, bit error rate is evaluated and compared with previous and proposed method. The number of bits error is divided by total number of bits transmitted in per unit time, also known as bit error ratio.

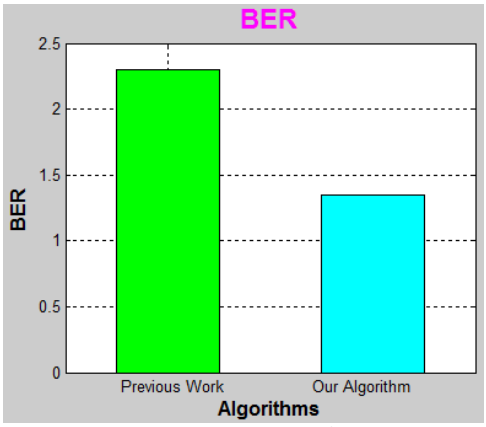


Figure 6, Comparison of ber

V.

VI. CONCLUSIONS

The present work first of all introduces this research was to compress an encrypted image in efficient way. Encryption technique focus on making changes to the original image in a manner that makes it invisible to attacker. Compression is used to reduce the size of image. The objective was to provide privacy as well as least possible storage space. The same has been achieved with transformation based compression using encryption but with a new algorithm of DAUBECHIES wavelet transform. Encrypting the image with random permutation method, results in distortion of image, which is visible to human eye. The research has resulted in a good mse, psnr, entropy, and ber. In future, entropy at global, local and conditional level may be evaluated for the better resolution.

ACKNOWLEDGMENT

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

REFERENCES

[1] R. C. Gonzalez and R. E. Woods, Digital Image Processing 2/E. Upper Saddle River, NJ: Prentice-Hall, 2002.

[2] J. J. Ding and J. D. Huang, "Image Compression by Segmentation and Boundary Description," June, 2008.

[3] G. K. Wallace, 'The JPEG Still Picture Compression Standard', Communications of the ACM, Vol. 34, Issue 4, pp.30-44.

[4] M. Campista, P. Esposito, I. Moraes, L. H. Costa, O. C. Duarte, D. Passos, C. V. de Albuquerque, D. C. Saade, and M. Rubinstein, outing metrics and protocols for wireless mesh networks, ‖ IEEE Netw., vol. 22, no. 1, pp. 6–12, Jan.–Feb. 2008.

[5] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, ―An efficient filter-based addressing protocol for auto configuration of mobile ad hoc networks,‖ in Proc. IEEE INFOCOM, Apr. 2009, pp.2464–2472.

[6] P. B. Velloso, R. P. Laufer, O. C.M. B. Duarte, and G. Pujolle, ―Trust management in mobile ad hoc networks using a scalable maturity based model, ‖ IEEE Trans. Netw. Service Manage. vol. 7, no. 3, pp. 172–185, Sep. 2010.

[7] D. Passos and C. V. N. Albuquerque, ―A joint approach to routing metrics and rate adaptation in wireless mesh networks, in Proc. IEEE INFOCOM Workshops, Apr. 2009, pp. 1–2.

[8] S. Biswas and R. Morris, ―ExOR: Opportunistic multi-hop routing for wireless networks,‖ in Proc. ACM SIGCOMM, Aug. 2005, pp. 133–143.

[9] Mitra, Y. V. SubbaRao, S. R. M. Prasanna, "A New Image Encryption Approach using Combinational Permutation Techniques"

[10]Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image" IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011.

[11] Daniel Schonberg, Stark C. Draper, Chuohao Yeo, KannanRamchandran, "Towards Compression of Encrypted Images and Video Sequences"

[12] Ibrahim Fathy El-Ashry, "Digital Image Encryption" A Thesis Submitted for The Degree of M. Sc. of Communications Engineering**.**

[13] D. Schonberg, S. C. Draper, C. Yeo, K. Ramchandran, "Toward compression of encrypted images and video sequences" IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 749–762, Dec. 2008.

[14] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," IEEE Trans. Inform. Theory, vol. IT-19, pp. 471–480, July1973.

[15]A.Wyner and J. Ziv, "The rate-distortion function for source coding withcside information at the decoder," IEEE Trans. Inform. Theory, vol. IT-22, cpp. 1–10, Jan. 1976.

[16] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," IEEE Trans. Inform.Theory, vol. 49, pp. 626–643, Mar. 2003.

[17] T. M. Cover and J. A. Thomas, Elements of Information Theory. NewYork: Wiley, 1991.

[18] M.W. Marcellin and T. R. Fischer, "Trellis coded quantization of memory less and Gauss-Markov sources," IEEE Trans. Commun., vol. 38, pp. 82–93, Jan. 1990.

[19]G. Ungerboeck, "Channel coding with multilevel/phase signals", IEEE Transaction Information Theory, vol. IT-28, pp. 55–67, Jan. 1982.

[20] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–175, 1949.

[21] A. D. Wyner, "The wire-tap channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.

[22] S. ParveenBanu, Dr.Y.Venkataramani, "An Efficient Hybrid Image Compression Scheme based on Correlation of Pixels for Storage and Transmission of Images" ,International Journal of Computer Applications (IJCA) (0975 – 8887)Volume 18– No.3, March 2011

[23]ManikGroach, Dr. AmitGarg, "DCSPIHT: Image Compression Algorithm", International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 2, Mar-Apr 2012, pp.560-567

[24] SandeepKaur, GaganpreetKaur and Dr.Dheerendra Singh, "Comparative Analysis of HaarandCoif let Wavelets Using Discrete Wavelet Transform in Digital Image Compression", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 3, May-Jun 2013, pp.669-673

[25] SherinKishk , HosamEldin Mahmoud Ahmed and HalaHelmy, "Integral Images Compression using Discrete Wavelets and PCA", International Journal of Signal Processing - Image Processing and Pattern Recognition, Vol. 4, No. 2, June, 2011.