ISSN:0975-9646

Designing an Efficient Image Encryption-Then-Compression System with Haar and Daubechies Wavelet

Harmanpreet Kaur Aujla, Rajesh Sharma

Computer Science, Punjab Technical University
Jalandhar, India

Abstract— Nowadays there is development in the multimedia and network technologies. That's why the privacy and security becomes the major issues since the multimedia is transmitted openly over the network .so that Along with privacy and security, the space of s storage is also an important point that can't be missed. So that, provide the privacy and security to the multimedia, encryption work as the similarly of root to reduce the storage space compression can be used. Reduction size also reducing the time taken for transmission. In many practical experiments, image encryption to be conducted prior to image compression. This has to be the problem, how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. In this research work, we design the algorithm and implement an efficient image encryption - compression system. The proposed image encryption method is operated with random permutation method which is shown to be providing reasonably high level of security. We also have implement the new kind of image compression algorithm using Haar and Daubechies Wavelet Transform can be used to efficiently compress the encrypted image. Moreover, the compression approach applied to encrypted image is proved more efficient in terms of Compression Ratio (CR), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR). For the implementation of this proposed work we use the Image Processing Toolbox under MATLAB software.

Keywords—ETC, Haar Wavelet and Daubechies Wavelet.

I.INTRODUCTION

The development of multimedia and network technologies, the security of multimedia application becomes more and more important, when the multimedia data are transmitted over open networks more and more frequently. Moreover, reliable security is necessary to content protection of digital images and videos. Encryption Techniques for multimedia data needs has to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. For example, the real-time encryption of an entire video stream 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, that can achieved using selective encryption that leaves some perceptual information after encryption. Government private business, and military, a mass great deal of confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), financial-status. Most of these information are now collected and stored on electronic computers and transmitted across network to other computer, if this confidential images about enemy positions ,patient ,and geographical areas fall into the wrong hands, After than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential images is an ethical and legal requirement. We store information in computer system in the form of files. Files are considered or defined as a basic entity for keeping the information. Then 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 look completely random, previous or traditional algorithms are unable 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. Neither the security nor the compression efficiency will be sacrificed by performing compression in the encrypted domain. **C**onsider an application scenario in which a content owner Alice wants to securely and efficiently transmit an image I to a recipient Bob, via an un-trusted channel provider Charlie. Conventionally, this could be done as follows. Alice first compresses I into B, and then encrypts B into I_e using an encryption function EK (·), where K denotes the secret key. The encrypted data I_e is then passed to Charlie, who simply forwards it to Bob. Upon receiving I_e, Bob sequentially performs decryption and decompression to get a reconstructed image I. Even though the above Compression-then-Encryption (CTE) paradigm meets the requirements in many secure transmission scenarios, order to applying the compression and encryption needs to be reversed in some other situations. As the content owner, always Alice is interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has to be no incentive to compress data, and will not use her limited computational resources to run a compression algorithm before encrypting the data, especially true when Alice uses a resource-deprived mobile device. In the contrast, channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. Therefore much desired if the compression task can be

delegated by Charlie, who can be typically has abundant computational resources. A big challenge within such Encryption-then-Compression (ETC) framework is that compression has to be conducted in the encrypted domain, as Charlie does not defined and access to the secret key K. This type of ETC system is demonstrated in Figure. The possibility of processing encrypted signals directly in the encrypted domain has been receiving increasing attention in recent years. At the first, it seems to be infeasible for Charlie to compress the encrypted data, since no signal structure can be exploited to enable a traditional compressor. Although counter-intuitive, Johnson showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency or the information-theoretic security. In addition to the theoretical findings, also proposed practical algorithms to losslessly compress the encrypted binary images. Schonberg later investigated the problem of compressing encrypted images when the underlying source statistics is unknown and the sources have memory. By applying LDPC codes in various bit-planes and exploiting the inter / intra correlation, Lazzeretti and Barni presented several methods for lossless compression of encrypted gray scale/color images.

II. HAAR WAVELET

In mathematics, the Haar wavelet is a sequence of rescaled "square-shaped" functions which together form a wavelet family or basis. The Wavelet analysis scheme is similar to Fourier analysis in that it allows a target function over an interval to be represented in terms of anorthonormal function basis. The Haar is sequence now recognized as the first known wavelet basis and extensively used as a teaching example in the theory of wavelets. The Haar wavelet is a certain sequence of functions. It is now recognized as the first known wavelet. This sequence was proposed in 1909 by Alfred Haar.

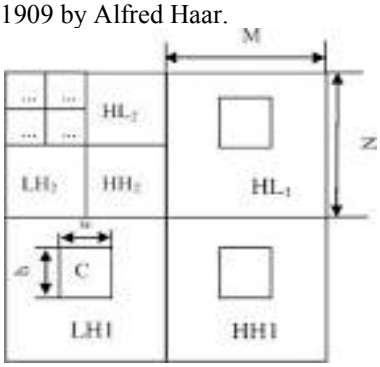


Figure 1. Haar wavelet

Haar technique is used these functions to give an example of a countable orthonormal system for the space of square integrable functions on the real line. The study of the wavelets, and even the term of "wavelet", did not come until much later. The Haar wavelet is also easier way to possible wavelet. Some of technical disadvantage of the Haar wavelet is that it is not continuous, and there not differentiable.

Haar transform or Haar wavelet transform has been used as an earliest example for orthonormal wavelet transform with compact support. The Haar wavelet family for $x \in [0, 1]$ is defined as follows:

$$h_i(x) = \begin{cases} 1 & \text{for} \quad x \in [\xi_1, \xi_2), \\ -1 & \text{for} \quad x \in [\xi_2, \xi_3], \\ 0 & \text{elsewhere} \end{cases}$$

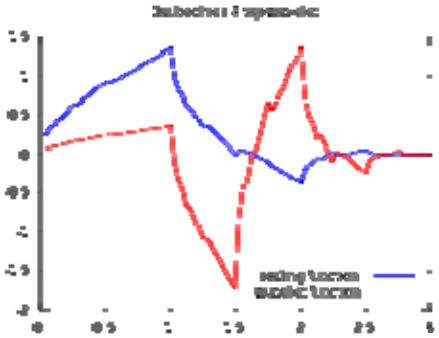
Here $\xi_1 = \frac{k}{m}, \xi_2 = \frac{k+0.5}{m}$ and $\xi_3 = \frac{k+1}{m}$.

In these formulae integer $m = 2^j$, $j = 0, 1, \ldots J$ indicates the level of the wavelet; $k = 0, 1, \ldots m - 1$ is the translation parameter. Maximal level of resolution is J and $2^J$is denoted as $M = 2^J$. The index i in is calculated from the formula $i = m + k + 1$; in the case of minimal values $m = 1$, $k = 0$ we have $i = 2$. The maximal value of i is $i = 2M = 2^{J+1}$. It is assumed that the value $i = 1$ corresponds to the scaling function for which $h_1(x) = 1$ in [0, 1]. It must be noticed that all the Haar wavelets are orthogonal to each other:

$$\int_0^1 h_i(x) h_l(x) dx = \begin{cases} 2^{-j} & i = l = 2^j + k \\ 0 & i \neq l \end{cases}$$

III. DAUBECHIES WAVELET TRANSFORM

The Daubechies wavelets, based on the work of Ingrid Daubechies, are the family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for some given support. With each type of that class, there is a scaling function (called the father wavelet) which generates an orthogonal Multi resolution analysis. In general the Daubechies wavelets are chosen to have the highest number A of vanishing moments, (this does not imply the better smoothening) for given support width N=2A. There are two naming schemes in use, DN using the length or number of taps, and db a referring to the number of vanishing moments. So D4 and db2 are the same wavelet transform. Among the 2^{A-1} possible solutions of the algebraic equations for the moment and orthogonality conditions, the one is chosen whose scaling filter has extremely phase. The wavelet transform is easier to put into practice using the fast wavelet transform. Daubechies wavelets are most of used in solving a broad range of problems, e.g. fractal problems or self-similarity properties of a signal, signal discontinuities, etc.



The Daubechies wavelets are not defined in terms of the resulting scaling and wavelet functions; in fact, that they are not possible to write down in closed form. The graphs below are generated using the cascade algorithm, a numeric technique consisting of simply inverse-transforming [1 0 0 0 0 ...] an appropriate number of times. Daubechies orthogonal wavelets D2-D20 resp. db1-db10 is commonly used. The index number refers to the number N of coefficients. Each wavelet has a multiples of zero moments or vanishing moments equal to half the number of coefficients. For example, D2 (the DAUBECHIES wavelet), D4 has two and has one vanishing moment etc. A vanishing moment limits the wavelets ability to represent polynomial behaviour or information in a signal. For example, the D2, one moment, easily encodes polynomials to one coefficient, and constant signal components. D4 encodes polynomials with two coefficients, i.e. constant and linear signal components; and D6 encodes 3-polynomials, i.e. constant, quadratic signal and linear components. This ability to encode signals is nonetheless subject to the phenomenon of scale leakage, and the lack of shift-invariance, which arise from the discrete shifting operation (below) during application of the transform. Sub-sequences which represent linear, quadratic (for example) signal components are treated differently by the transform depending on whether the points align with even- or odd-numbered locations in the sequence. The lack of the important property of shift-invariance, has led to the development of several different versions of a shift-invariant (discrete) wavelet transform.
There are some parameters given which is useful in our implementation.

A. MSE:

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

$$MSE = (1/N)\Sigma i|x(i)- e(i)|^2 \quad (4)$$

Here x and e are encrypt to watermarked audio signals respectively and N is the number of samples in the audio signal.

B. PSNR

Embedding this extra data must not degrade human perception about the object. Namely, the watermark should be “invisible” in a watermarked image or “inaudible” in watermarked digital music. Evaluation of the imperceptibility is that usually based on an objective measure of quality, called peak signal to noise ratio (PSNR), or a subjective test with specified procedures. The PSNR values can be obtained using following formula:

$$PSNR = 20\log10 (PIXEL\_VALUE/\sqrt{MSE}) \quad (5)$$

IV. OBJECTIVE

In this thesis, we propose ‘designing an Efficient Image Encryption-Then-Compression System with HAAR and DAUBECHIES Wavelet Transform’. The main objective of the project is to discuss the properties which help to transmit the secret message or information over a network without any modifications.

The characteristics of information are following:
1) Availability
2) Accuracy
3) Authenticity
4) Confidentiality
5) Integrity

Our objective is to develop a high performance compression system. The design of such system mainly consists in the optimization of the following attributes:

- The compression ratio, used to quantify the reduction in image-representation size produced by a compression algorithm. It is defined as the ratio of the size of the compressed signal to that of the initial signal.
- The accuracy with which the compressed signal can be recovered at the receiver. Different Efficient techniques are to be developed to minimize the impact of compression on the image.
- We use Image Compression using Encryption Then Compression with Haar and DAUBECHIES wavelet thus providing two tier compressions.
- Even if image is tampered with our compressed image doesn't get distorted and thus our purpose is fulfilled.
- Better PSNR and compression ratio results of Encryption Then Compression with Haar and DAUBECHIES wavelet.

V. EXPERIMENTAL RESULT

In this phase, present results are better of the experiments to corroborate the success of the proposed model.

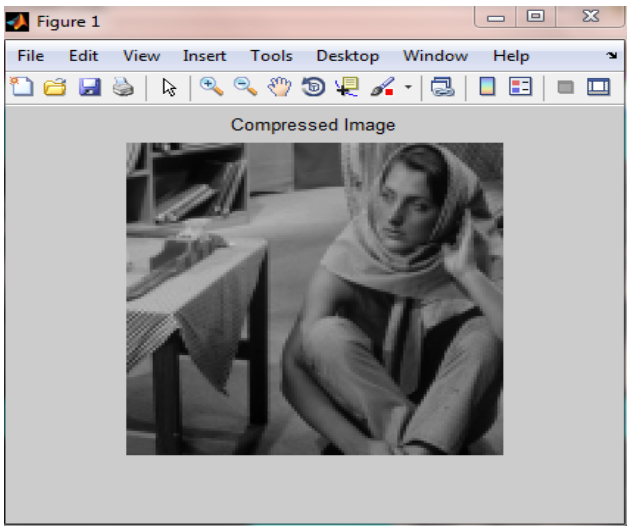
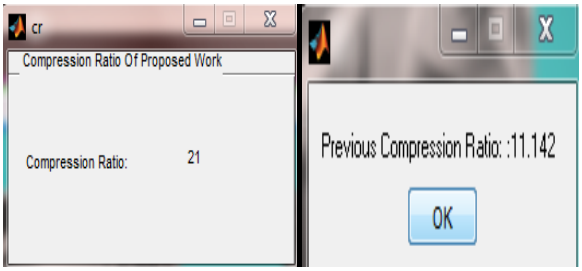


Figure 1: Compressed Image



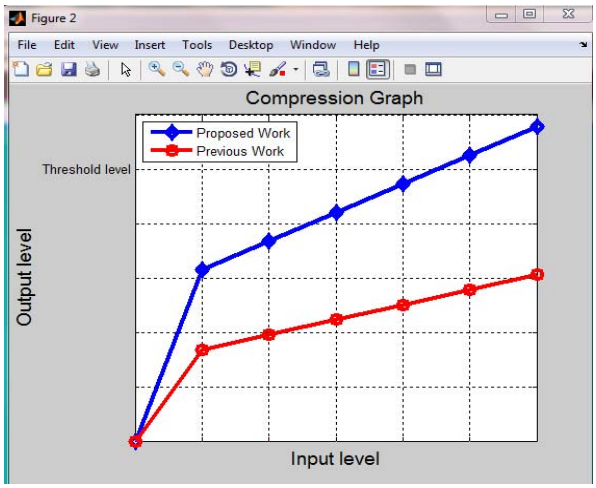


Figure 2: Compression Graph

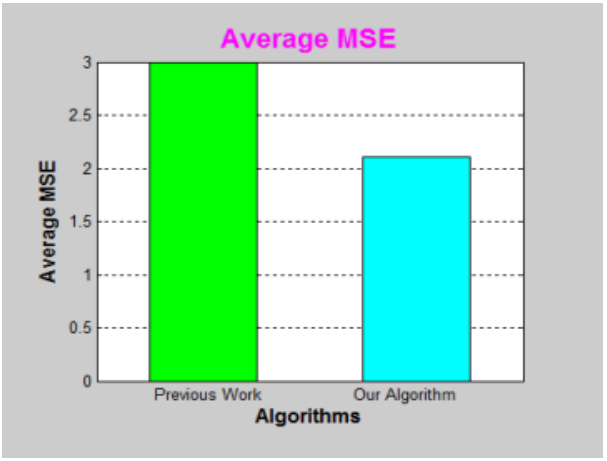


Figure 3: MSE Graph

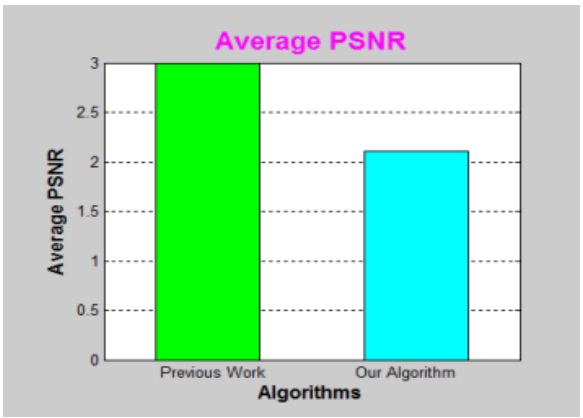


Figure 4: PSNR Graph

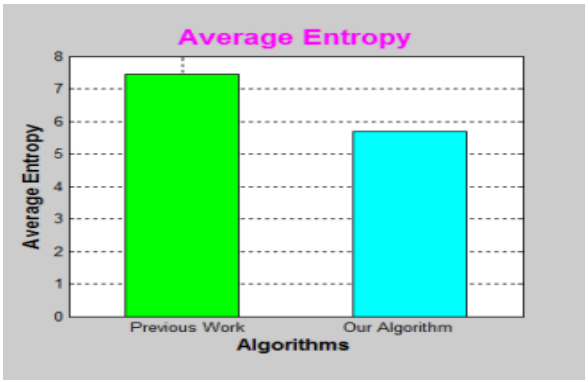


Figure 5: Entropy Graph

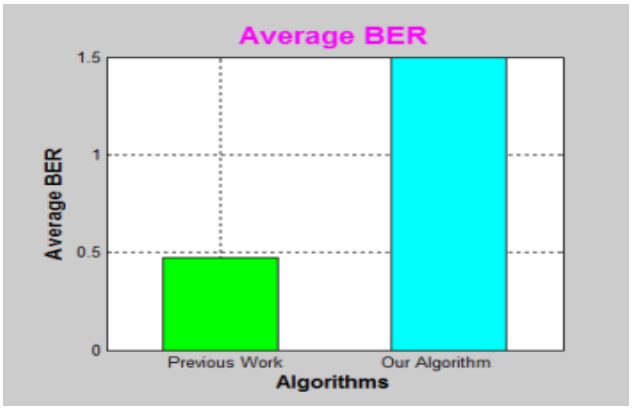


Figure 6: BER Graph

VI. CONCLUSION

In this research work, we have designed an efficient image Encryption-Compression system. Within the proposed framework, the image encryption has to be achieved via random permutation. Highly efficient compression of encrypted image has been realized by a new image compression algorithm of Haar and Daubechies wavelet transform. To proposed 'designing an Efficient Image Encryption-Then-Compression System with HAAR and DAUBECHIES Wavelet Transform'. Then encrypt image using pseudo random permutation. In this method the pixel values are same after encryption but their position will be changed. The image obtained is nearly similar to the original image due to high correlation between the adjacent pixels. Then compression of encrypted images, majority of pixels are converted to a series of coefficients using an orthogonal transform, and after then the fine information and excessively rough in the coefficients is removed, leading to a reduced data amount. Many Image Compression techniques have been proposed earlier but they were not secure enough and compression ratio is poor. Image Compression could not provide better results as technique used for Compression with DAUBECHIES wavelet alone was not good enough. Therefore Haar wavelet used with Daubechies wavelet for data compression. And propose 'designing an Efficient Image Encryption-Then-Compression System with HAAR and DAUBECHIES Wavelet Transform. In future the same technique can be extended by applying different transforms to cover image and thus robustness of algorithm can be verified.

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. Subba Rao, 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, Kannan Ramchandran, "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, July 1973.

[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. New York: 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 Trans. Inform. 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.