International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

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

Ambika[1], Neha[2]

[1,2]Computer Science, Himachal Pradesh Technical Universityl, India

Abstract: ***Images can be encrypted with different ideas which is a modified International DAUBECHIES ,SYMLET and HAAR Wavelet with Data Encryption Algorithm to encrypt the full image in an efficient secure way, after encryption the original file will be compressed and get compressed image. The ideas of image encryption scheme operated in the prediction error domain are shown to be able to provide a reasonably high level of security. Here also find that an arithmetic coding-depend approach can be exploited to efficiently compress the encrypted image. In contrast, the existing ETC solutions induce significant penalty on the compression efficiency. Haar, SYMLET and DAUBECHIES wavelet transform using with ETC perform better compression efficiency.***

Keywords: - Haar wavelet, Daubechies wavelet and Encryption-Then-Compression, SYMLET

1. Introduction

With the fast growing in multimedia and network technologies; the security of multimedia becomes more important. Since, multimedia information is transmitted over open networks more frequently. Typically; the reliable security is necessary to data protection of digital figures and videos. Encryption techniques for multimedia information need to be specifically designed to save multimedia information and fulfil the security need for a particular multimedia application. Take example; real-time encryption of an entire video stream using classical ciphers needs heavy computation due to the more amounts of data involved; but many multimedia applications require security to a lower level; this can be gained using selective encryption that leaves some perceptual message after encryption. Therefore Government; military and private business amass great deal of confidential figures. Most of information is collected and stored on electronic computers and transmitted across network to other computer, if these confidential figures about enemy positions, patient, and geographical areas goes to the wrong

Hands; than such a breach of security could lead to more wars, wrong treatment etc. Protecting confidential figures is an Ethical and legal requirement. We store data in computer system in the form of files. File is taken as a basic entity for keeping the information. It is worldwide accepted fact that securing file data is very important in computing environment. Best encryption makes a source look completely random; traditional algorithms are unable to compress encrypted data. To this reason, traditional systems make sure to compress before they encrypt. Here 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. The possibility of processing encrypted data directly in the encrypted domain has been receiving increasing attention in recent years. At the first glance; this seems to be infeasible for Charlie to compress the encrypted information, 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 finding; and invented practical algorithms to lossless compress the encrypted binary figures. Schonberg later investigated the problem of compressing encrypted figures when the underlying source statistics is unknown and the sources have memory.

2. Haar Wavelet

The **Haar wavelet** is a certain sequence of functions which is now recognised as the first known wavelet. This sequence was proposed in 1909 by Alfred Haar.

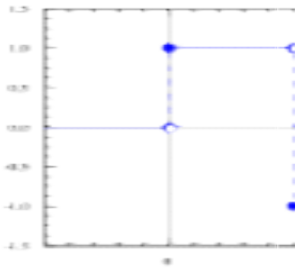

Figure 1: Haar wavelet window

Haar used these functions to give an example of a countable orthonormal system for the space of square integral functions on the real line. The study of wavelets and the term "wavelet", did not come until much later. The Haar wavelet is also the simplest wavelet. The Haar wavelet has a technical disadvantage is that it is not continuous and not differentiable.

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

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

Scaling function φ (*t*) can be described as:

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

Wavelets are mathematical functions that were developed by scientists working in several different fields for the purpose of sorting data by its frequency. Then the Translated data can be sorted at a resolution which matches its scale. At different levels, the Studying data allows for the development of a more complete picture. By this, both small features and large features are discernable because they are studied separately. After that, the wavelet transform is not Fourier-based and therefore wavelets do a better job of handling discontinuities in data. The Haar wavelet operates on data by calculating the sums and differences of elements which are adjacent. 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 :

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3)$$

3. Daubechies Wavelet Transform

The Daubechies wavelets, are a family of orthogonal wavelets defining a discrete wavelet transform and characterized by a maximal number of vanishing moments for the given support. From each wavelet type of this 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, for given support width N=2A. There are two main naming schemes in use. The DN using the length or number of taps, and db a referring to the number of vanishing moments. So, both 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 wavelet transform is very easy to put into the practice using the fast wavelet transform. The Daubechies wavelets are widely used to solve a broad range of problems, e.g. self-similarity signal properties or fractal problems, signal discontinuities, etc.

The Daubechies wavelets are not defined in terms of the resulting scaling and wavelet functions. In fact, they are not possible to write down in the closed form. The following graphs 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. In this, Each wavelet has a number of zero moments or vanishing moments equal to half the number of coefficients. For example, D2 (the DAUBECHIES wavelet) has one vanishing moment, D4 has two vanishing moments, etc. A vanishing moment limits the wavelets ability to represent polynomial behaviour or information in the signal. Sub-sequences which represent linear, quadratic 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 vital property of shift-invariance has led to the development of several different versions of a shift-invariant wavelet transform.

4. Symlet Wavelet Transform

Symlet wavelets are a family of wavelets. They are a modified version of Daubechies wavelets with increased symmetry. Symlets are also orthogonal and compactly supported wavelets, which are proposed by I. Daubechies as medications to the db family. Symlets are near symmetric and have the least asymmetry. The associated scaling filters are near linear-phase filters. The properties of Symlets are nearly the same as those of the db wavelets. There are some parameters which are useful in our implementation:

A. MSE:-

Mean Squared Error is essentially a signal exactness measure. The goal of a signal exactness measure is to compare two signals by providing a quantitative score that describes the degree of exact or conversely. Usually, it is assumed that one of the signals is a intact original, while the other is distorted by errors. The MSE between the images is given by using the following formula:

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

Here, 'x' and 'e' are the compressed and original images respectively and the N is the size of image.

B. PSNR:-

Compressing this extra data must not degrade human perception of an object. Evaluation of insensible is 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:

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

The 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 end. The 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, DAUBECHIES and Symlet wavelet thus providing three 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, DAUBECHIES and Symlet wavelet.

5. Conclusion

To proposed 'designing an Efficient Image Encryption-Then-Compression System with HAAR , DAUBECHIES and Symlet Wavelet Transform'. 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 compressions of encrypted images, majority of pixels are converted to a series of coefficients using an orthogonal transform. Then the excessively rough and fine information 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 and Symlet wavelet for data compression. And propose 'designing an Efficient Image Encryption-Then-Compression System with HAAR, DAUBECHIES and Symlet Wavelet Transform'.

6. 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