International Journal of Engineering Research and General Science Volume 4, Issue 2, March-April, 2016
ISSN 2091-2730

Designing of an efficient image encryption-compression system using a New Haar and Coiflet with Daubchies and Symlet wavelet transforms

Savita Devi, Astha Gautam(Assistant Professor)

Department of CSE, LRIET Solan,savitasharma.b@gmail.com

Abstract - The security of multimedia becomes more important, since multimedia data are transmitted over open networks more frequently. In this modern world, hidden information concept are very important and play a significant role to reducing the space in the memory as well as on disk drives. Compression of the encrypted information has taken more attention due to security reasons from last few years. If encryption and compression of the information works properly then it results to high speed computation. According to practical scenario encryption should be performed before the compression of information. Because unencrypted information have more chances of stealing. And now a day's data hacker becomes too intelligent to break the encrypted images to get the original contents, so many systems are designed to combine the encryption and compression in single module to provide greater security. Therefore we have proposed system where encryption is done prior to the image compression by random permutation method and after that we can efficiently compress the encrypted image. In this paper, we study a new approach is named as ECNHCDSWT (Encryption-Compression using New Haar and Coiflet with Symlet and Daubchies wavelet transform).

Keywords –Encryption, Compression, ETC, Haar, Coiflet, Symlet, Daubchies, CR, MSE, PSNR.

1. INTRODUCTION

The security of multimedia becomes more important, since multimedia data are transmitted over open networks more frequently. Typically, reliable security is necessary to content protection of digital images and videos [2]. Encryption and compression schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. Image Encryption means that convert an image to unreadable format so that it can be transmitted over the network safely. Image Decryption means to convert the unreadable format of an image to original image. This is used to protect the secrets of corporate as well as government's offices. [1].

Compression: It is done in order to save storage space or transmission time. The purpose of compression is reduction in size. The main objective behind compressing an image is to reduce the unimportant and redundant data, so as to store or transmit data in more efficient way. The applications of data compression in diverse areas re as follows:

- Satellite imagery
- Mini discs
- MP3technology
- Modems
- Digital cameras
- Database Design
- Storage and transmission of data
- Distributing Software
- Data Transmission

Image compression addresses the problem of reducing the amount of data required to represent a digital image. It is a process intended to yield a compact representation of an image, thereby reducing the image storage/transmission requirements [3]. Compression is achieved by the removal of one or more of the three basic data redundancies:

- Coding Redundancy
- Interpixel Redundancy
- Psychovisual Redundancy

The image compression techniques are broadly classified into two categories depending whether or not an exact replica of the original image could be reconstructed using the compressed image.

These are:

- Lossless technique
- Lossy technique

Lossless compression technique

In lossless compression techniques, the original image can be perfectly recovered from the compressed (encoded) image. These are also called noiseless since they do not add noise to the signal (image). It is also known as entropy coding since it use

statistics/decomposition techniques to eliminate/minimize redundancy. Lossless compression is used only for a few applications with stringent requirements such as medical imaging.

Lossy compression technique

Lossy schemes provide much higher compression ratio than lossless schemes. Lossy schemes are widely used since the quality of the reconstructed images is adequate for most applications .By this scheme, the decompressed image is not identical to the original image, but reasonably close to it.

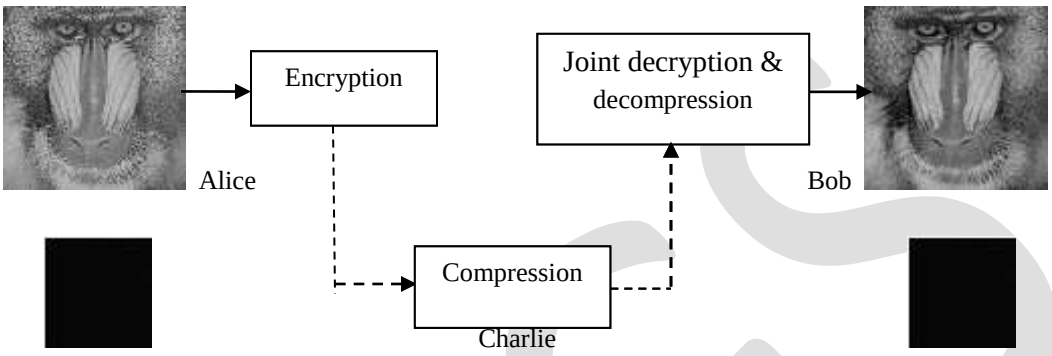

Fig. 1. Encryption-Then-Compression System

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, whereas frequency analysis is performed with a dilated, low-frequency version of the same wavelet.

2.1 Discrete Haar Wavelet Transform (DHWT)

An outstanding property of the Haar functions is that except function Haar (0, t), the i^{th} Haar function can be generated by the restriction of the $(j-1)^{th}$ function to be half of the interval where it is different from zero, by multiplication with $\sqrt{2}$ and scaling over the interval [0, 1]. These properties give considerable interest of the Haar function, since they closely relate them to the wavelet theory. In this setting, the first two Haar functions are called the global functions, while all the others are denoted as the local functions. Hence, the Haar function, which is an odd rectangular pulse pair, is the simplest and oldest wavelet. The motivation for using the discrete wavelet transform is to obtain information that is more discriminating by providing a different resolution at different parts of the time–frequency plane. The wavelet transforms allow the partitioning of the time-frequency domain into non-uniform tiles in connection with the time–spectral contents of the signal. The wavelet methods are strongly connected with classical basis of the Haar functions; scaling and dilation of a basic wavelet can generate the basis Haar functions.

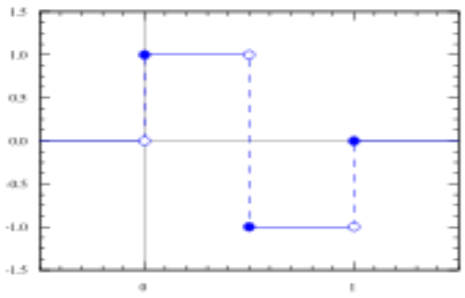

Fig. 2. Haar function on real line [2]

The Haar wavelet operates on data by calculating the sums and differences of adjacent elements. The Haar wavelet operates first on adjacent horizontal elements and then on adjacent vertical elements. Then it operated transformation coding and then encoding steps take place. For the retrieval of original image inverse process needs to follow so that the reconstruction of image can take place.

2.2 Coiflet Wavelet

Coiflets are discrete wavelets designed by Ingrid Daubchies, at the request of Ronald Coifman, to have scaling functions with vanishing moments. The wavelet is near symmetric; their wavelet functions have $N/3$vanishing moments and scaling functions $N/3-1$, and have been used in many applications using Calderón-Zygmund Operators.

Both the scaling function (low-pass filter) and the wavelet function (High-Pass Filter) must be normalized by a factor$1/\sqrt{2}$. Below are the coefficients for the scaling functions for C6-30. The wavelet coefficients are derived by reversing the order of the scaling function coefficients and then reversing the sign of every second one (i.e. C6 wavelet = {−0.022140543057, 0.102859456942, 0.544281086116, −1.205718913884, 0.477859456942, 0.102859456942}). Mathematically, this looks like $\mathbf{B_k = (-1)^k C_{N-1}}$ where *k* is the coefficient index; *B* is a wavelet coefficient and *C* a scaling function coefficient. *N* is the wavelet index, i.e. 6 for C6. A biorthogonal wavelet is a wavelet where the associated wavelet transform is invertible but not necessarily orthogonal. Designing biorthogonal wavelets allows more degrees of freedom than orthogonal wavelets. One additional degree of freedom is the possibility to construct symmetric wavelet functions. In the biorthogonal case, there are two scaling functions $\phi, \tilde{\phi}$, which may generate different multi resolution analyses, and accordingly two different wavelet functions $\psi, \tilde{\psi}$. So the numbers *M* and *N* of coefficients in the scaling sequences $a, \tilde{a}$may differ. The scaling sequences must satisfy the following biorthogonality condition

$$\sum_{n\in\mathbb{Z}} a_n \tilde{a}_{n+2m} = 2 \cdot \delta_{m,0}$$

.

Then the wavelet sequences can be determined as

$$b_n = (-1)^n \tilde{a}_{M-1-n} \qquad (n = 0, \ldots, N-1)$$

$$\tilde{b}_n = (-1)^n a_{M-1-n} \qquad (n = 0, \ldots, N-1)$$

.In *coif N*, *N* is the order.

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/ √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.

2.3 Symlet Wavelet

Symlet wavelets are a family of wavelets. They are a modified version of Daubchies wavelets with increased symmetry. In *symN*, *N* is the order. Some authors use 2*N* instead of *N*. Symlets are only near symmetric; consequently some authors do not call them symlets. More about symlets can be found in [Dau92], pages 194, 254-257. By typing waveinfo('sym') at the MATLAB command prompt, you can obtain a survey of the main properties of this family [11].

2.4 Daubchies

Daubchies proposes modifications of her wavelets that increase their symmetry can be increased while retaining great simplicity.

The idea consists of reusing the function m_0 introduced in the *dbN*, considering the $|m_0(\omega)|^2$ as a function *W* of $z = e^{i\omega}$.

Then we can factor *W* in several different ways in the form of $W(z) = U(z)\overline{U\left(\frac{1}{z}\right)}$ because the roots of *W* with modulus not equal to 1 go in pairs. If one of the root is z_1, then $\frac{1}{z_1}$ is also a root.

- By selecting *U* such that the modulus of all its roots is strictly less than 1, we build Daubchies wavelets *dbN*. The *U* filter is a "minimum phase filter."
- By making another choice, we obtain more symmetrical filters; these are symlets.

The symlets have other properties similar to those of the *dbN*s.

2.5 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

Encryption-Compression using New Haar, Coiflet, Symlet and Daubchies wavelet transform (ECNHCSNDWT)

The input image has been considered as 'I', encryption over 'I' has been implemented using random permutation method. The obtained result after encryption has been considered as 'I_e', and then a new Haar, Coiflet, Symlet and Daubchies wavelet technique has been used for compression. The output after compression has been stored as image 'B'. Then the image 'B' has been decrypted after decompression. [1]

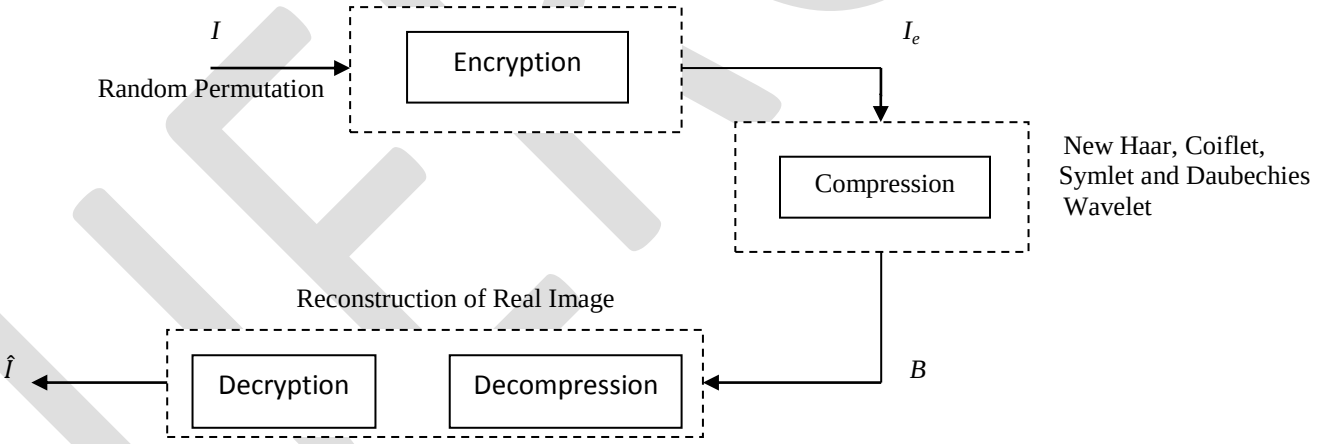

Fig. 3. Proposed Model for Encryption-Compression System

As shown in Fig. 3. Encryption-Compression system is proposed. The resultant image Î is evaluated using various parameters like CR, MSE and PSNR to check the efficiency and to compare it with the result of existing system. We can also represent the proposed schema with the help of flowchart. Fig.4. Shows the flowchart that represents the procedure flow of various steps. Half of the flowchart represents the encryption steps and rest represents the compression steps. Then inverse process to retrieve the real image and then calculation steps to check the efficiency.

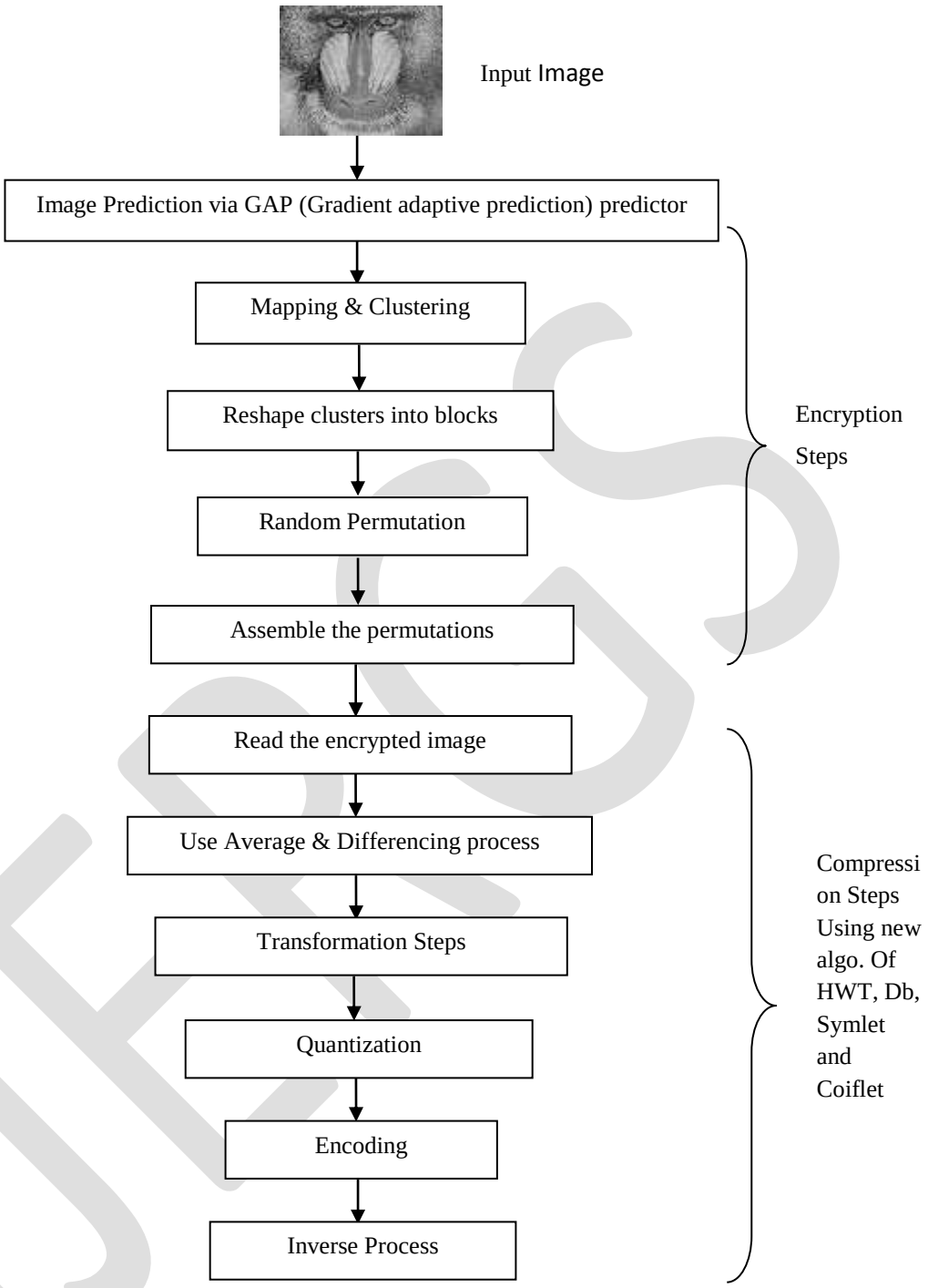

Fig. 4. Flowchart for Image Encryption-Compression Scheme [1]

5. RESULTS EVALUATION

In this section, we will perform experiment to verify the efficiency of our approach. The comparison of the accuracy is done for every method is one with the given values to the proposed work. With our approach result will evaluated with different parameters as CR (compression ratio), MSE (mean square error) and PSNR (peak signal to noise ratio).

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] 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.

[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] 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, issue 11, Nov. 2012.

[6] 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.

[7] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images", IEEE Trans. Imag. Process, vol. 21, issue 6, June 2012.

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

[9] X. Zhang, Y. L. Ren, G. R. Feng, and Z. X. Qian, "Compressing encrypted image using compressive sensing", in Proc. IEEE 7th IIH-MSP, Oct. 2011.

[10] M. Barni, P. Failla, R. Lazzeretti, A. R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks", IEEE Trans. Inf. Forensics Security, vol. 6, issue 2, June 2011.

[11] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image", IEEE Trans. Inf. Forensics Security, vol. 6, issue 1, Mar. 2011.

[12] W. Liu, W. J. Zeng, L. Dong, and Q. M. Yao, "Efficient compression of encrypted grayscale images", IEEE Trans. Imag. Process, vol. 19, issue 4, Apr. 2010.

[13] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals", IEEE Trans. Inf. Forensics Security, vol. 5, issue 1, Mar. 2010.