

**Encryption-then-Compression System using
Haar and Symlet Wavelet Transform**

A Dissertation
Submitted

By

Navneet Kaur

To

Department of

Computer Science & Engineering

In partial fulfilment of the Requirement for the

Award of the Degree of

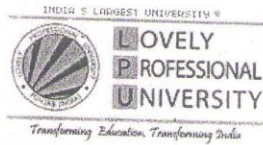
**Master of Technology in Information
Technology**

Under the guidance of

Mr. Sanyam Anand

(May 2015)

PAC FORM



School of: Computer Science & Engineering

DISSERTATION TOPIC APPROVAL PERFORMANCE

Name of the Student: NAVNEET KAUR Registration No: 11309778
Batch: 2013-15 Roll No:
Session: 2014-15 Parent Section: K2308
Details of Supervisor:
Name: SANYAM Designation: AP
U.ID: 15736 Qualification: M.Tech (IT)
Research Experience: 2 years

SPECIALIZATION AREA: DIGITAL IMAGING (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Medical Image Compression & Enhancement using Wavelets
2. Image Forensics & Security
3. Image denoising

[Signature]
Signature of Supervisor

PAC Remarks:

Topic 1 is approved.

[Signature]
11/01/15

APPROVAL OF PAC CHAIRPERSON:

Signature:

Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Image compression is the important task for the medical images. Economic and effective image compression techniques are hardly required to minimize the storage volume of medical database in hospitals as well as maintaining the image quality. But the transmission and storage of such a large data could be a tedious job. There are various methods to encrypt the images while transmission. In this research, the proposed system is Encryption then Compression of medical images where Haar and Symlet wavelets can be exploited to efficiently compress the encrypted images. The proposed encryption technique is conducted on the basis of Prediction Error Clustering and Random Permutation to provide the high security at the transmission and the compression of the encrypted image is operated by the Haar and Symlet wavelets. The greater compression efficiency is expected at the compression of the encrypted image with high level of security.

CERTIFICATE

This is to certify that Navneet Kaur has completed M.Tech dissertation titled, “**Encryption-then-Compression System using Haar and Symlet Wavelet Transform**” under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation has ever been submitted for any other degree or diploma. The dissertation is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science &Engineering.

Date: _____

Signature of Advisor

Name: Sanyam Anand

UID: 15736

ACKNOWLEDGEMENT

First and foremost I would like to thank almighty for giving me courage to bring up this dissertation. Before getting into thick and thin of this dissertation I would like to show my gratitude to some of the people who have helped me in this project.

Firstly I would like to propose a word thanks to my mentor Mr. Sanyam Anand who has encouraged me to get through this dissertation. Secondly I would like to thanks my friends who gave me unending support and helped me in numerous ways from the stage when the idea of the thesis was conceived.

I am very thankful to all of them for making my work complete successfully under their guidance.

Navneet Kaur

Reg.No.11309778

DECLARATION

I hereby declare that the dissertation entitled, "Designing an efficient Encryption-then-Compression System using new Haar and Symlet Wavelet Transform" submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: _____

Investigator: Navneet Kaur

Regd. No.:11309778

TABLE OF CONTENTS

Abstract	i
Certificate	ii
Acknowledgement	iii
Declaration	iv
Table of contents	v
List of Tables	vii
List of Figures	viii
CHAPTER 1: INTRODUCTION	1
1.1. Image Representation	2
1.2. Image Encryption	3
1.2.1. Image Encryption Techniques	4
1.2.2. Random Permutation Method	4
1.3. Encryption-then-Compression System	4
1.3.1.Prediction Error Domain and Random Permutation	5
1.3.2.Gradient adjusted predictor (GAP)	6
1.3.3.Column and Row Shift Operation	7
1.4. Image Representation	8
1.4.1. Wavelet Transform	9
1.4.1.1 Haar Wavelet	10
1.4.1.2 The Haar function	10
1.4.1.3 Symlet Wavelets	12
1.5. Evaluation Parameters	13
CHAPTER 2: LITERATURE REVIEW	15
CHAPTER 3:PRESENT WORK	25

3.1.Objectives	25
3.2. Problem Formulation	26
3.3. Work Methodology	27
3.4. Software used	30
CHAPTER 4: RESULTS AND DISCUSSION	33
4.1 Results	33
4.2 Graphs	41
CHAPTER 5: REFERENCES	45
CHAPTER 6: APPENDIX	49
7.1. Abbreviations	49
CHAPTER 7: PUBLICATIONS	50

List of Tables

Table 1.1	Encryption of Images	3
Table 1.2	Lists of Compressed Images	9
Table 4.1	Layout of various resultant Images	37
Table 4.2	CR, MSE, and PSNR	38
Table 4.3	CR, MSE, and PSNR	39
Table 4.4	Comparison of BER and the Entropy with the existing system	39
Table 4.5	Comparison of PSNR with the existing system	40
Table 4.6	Comparison of BER and the Entropy with the existing system	40

List of Figures

Fig.1.1	Pixel Representation	2
Fig.1.2	Pixel values for different colors	2
Fig.1.3	Block Diagram of Random Permutation Method	4
Fig.1.4	Encryption-then-Compression System	5
Fig.1.5	Schematic Diagram of Image Encryption	6
Fig.1.6	Gradient Adjusted Predictor	6
Fig.1.7	An Example of Cyclical Shift	8
Fig.1.8	Block Diagram of Image Compression	8
Fig.1.9	Haar wavelets	10
Fig.1.10	Symlet Functions	13
Fig.3.1	Proposed Model for Encryption-Compression System	27
Fig.3.2	Flowchart of Image Encryption-Compression Scheme	29
Fig.3.3	Software used- MATLAB	30
Fig.4.1	Gray-scale Images	33
Fig.4.2	Encryption of synpic2712 (a)-(b)	34
Fig.4.3	Compression of Encrypted Image	35
Fig.4.4	Reconstruction of Real Image	36
Fig.4.5	Compression Graph	40
Fig.4.6	Solidity Graph	40
Fig.4.7	PSNR Graph	41
Fig.4.8	MSE Graph	41
Fig.4.9	Entropy Graph	42
Fig.4.10	BER Graph	42
Fig.4.11	Graph of various parameters	42

CHAPTER 1

INTRODUCTION

Medical images are very important in the field of medicine. Many of medical imaging techniques such as Computed Tomography (CT) are used to develop the medical images, produce a sufficient data which requires a large storage area. An average 12-bit X-ray image is nearly 2048 pixels by 2560 pixels dimensionally, converting to a file of size 10,485,760 bytes. An expressive transmission cannot be achieved if the image compression is not efficient, which helps in reducing the file sizes at the same time preserving the image quality. At first, the compression of medical images begun with using the image preservation techniques such as Scan pixel difference, which is pursued by intra and inter-frame redundancy reduction considered linear. The main challenge coped by medical compression techniques is that there is constant change in the imaging devices and as they used the different techniques to produce the medical images, so the new compression techniques are required. Comprehensively, there are two compression techniques described as follow:

Lossless Compression: In the lossless compression technique, when the decompression of compressed image is conducted, the image retrieved is same as the original image before compression.

Lossy Compression: In the case of lossy compression technique, the image which is compressed if decompressed, the image retrieved is not same as the original image before compression, some of information is lost. The compression ratio of the lossy technique is more than the lossless technique. But the lossy compression techniques are not used extensively in medical imaging. There may be the loss of data which contains useful information, affecting the diagnosis of the patient.

An expressive transmission cannot be achieved if the image compression is not efficient, which helps in reducing the file sizes at the same time preserving the image quality.

1.1 Image Representation

All the images comprise of pixels which have values in twofold or byte, having rectangular lattice of pixels that have fixed height and a clear width evaluated in pixels where as every pixel is square and has a settled size on a given display. Different PC screens may utilize distinctive measured pixels where every pixel has a color which is a 32-bit integer. The initial 8-bits focus the visibility of pixel which indicates in Fig. 1.1, where next 8-bits the redness, next 8-bits the greenness and the following 8-bits the blueness and image spoke to, for every single numerical purpose as a lattice.

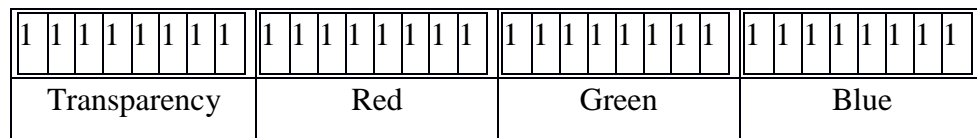


Fig. 1.1 Pixel Representation

Every can be translated as an unsigned byte around 0 and 255 with shading higher numbers are brighter. There is Red of 0 methods no red at all while a red of 255 is a splendid red. 1 value through 254 is dealt with as totally straightforward. Different hues are made by combining distinctive levels of the three essential hues e.g., gray is 127 red, 127 green, and 127 blue are gray.

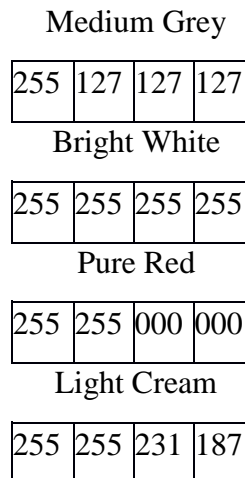


Fig. 1.2 Pixel values for Different colors

1.2 Image Encryption

These days, when more sensible information is kept on computer and transmitted over the web, ought to guarantee the data security. As all realize that image is likewise a critical piece of this data. Along these lines, it is vital to shield our image from unapproved access. Fundamentally, Image Encryption implies that change over a image to disjointed unrecognizable format so it can be transmitted over the network securely. Image Decryption intends to recover the original image from the unreadable format.

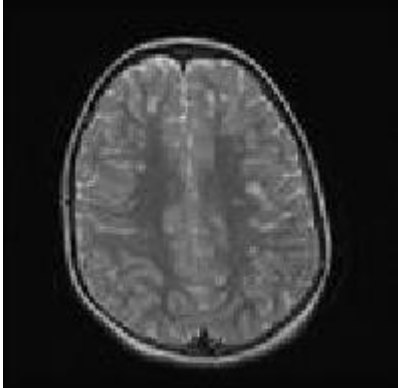

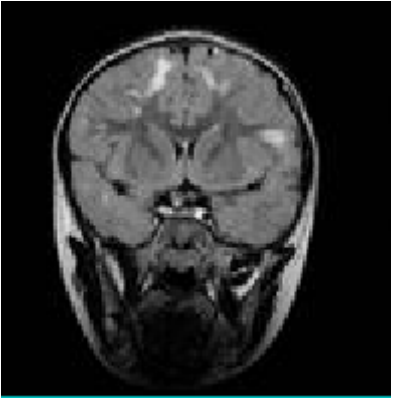

 <p>Original Image</p>	 <p>Encrypted Image</p>
 <p>Original Image</p>	 <p>Encrypted Image</p>

Table 1.1 Encryption of images

Fig. 1.3 shows that the encryption of an image. The output showed in Fig. 1.3 can be evaluated by utilizing several image encryption techniques.

1.2.1 Image Encryption Techniques

- DCT Based techniques are compression oriented e.g., Zig-Zag Permutation.
- Wavelet based techniques are also compression oriented e.g., Coefficient Selective Bit Encryption.
- Advanced Techniques are based on two main factors i.e., Raw Image data and Block based where raw image data is based on Permutations

1.2.2 Random Permutation Method

Symmetric cryptography procedure uses a Pseudo random index generator for formation of keys. The three fundamental permutation methods are bit permutation, to encrypt image, block permutation and pixel permutation are utilized in any order.

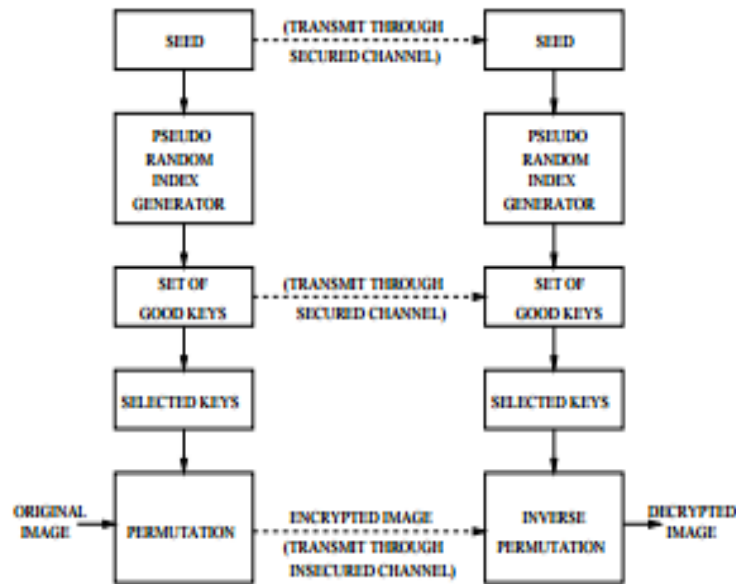


Fig. 1.3 Block Diagram of Random Permutation Method

1.3 Encryption –Then –Compression System

As the network technologies are developing fast, the reliable security at the transmission of the data is necessary. It needs a encryption of transferring data, various encryption methods are designed to provide the security to data which is to be transmitted. Consider an example where the Alice wants to transmit the image I to Bob through a channel provider Charlie.

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

Alice first encrypted the image I into I_e and using encryption method where the secret key is K . After that, the encrypted image I_e is then transferred to the channel provider Charlie. Charlie then compressed the encrypted image I_e into B and forwards the image B to Bob. After receiving B , Bob operates decompression to get the I_e which is then decrypted to get the reconstructed image [6]. The above Encryption-Then-compression (ETC) system is shown in Figure below

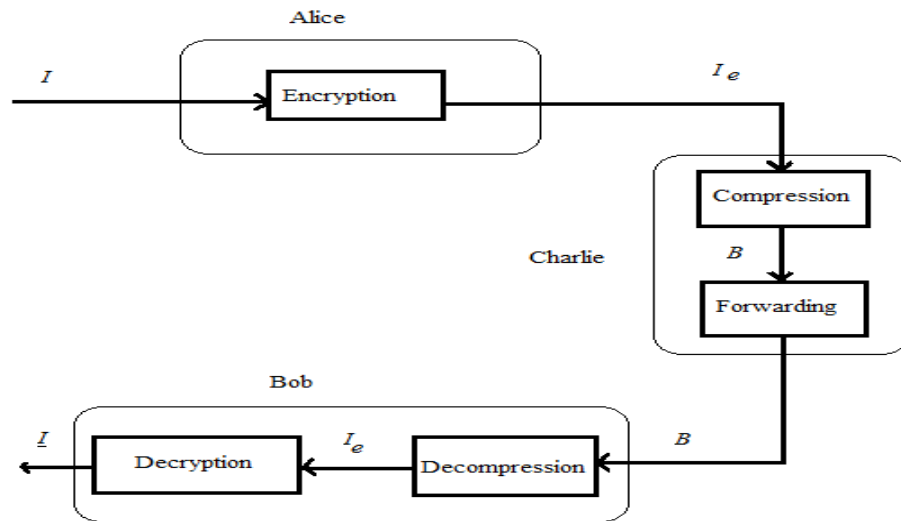


Fig. 1.4 Encryption-then-Compression System

1.3.1 Prediction Error Domain and Random permutation

The image encryption is conducted using prediction error domain.

- For every pixel $I_{i,j}$ of the image I that has to be encrypted, the predicted pixel value is predicted by using any image predictor like GAP[] or MED[], as per the surrounding values. The predicted result is further refined through a context-adaptive, feedback mechanism.
- Then the prediction error is conducted by computing the error domain $e_{i,j} = I_{i,j} - \hat{I}_{i,j}$ which is then clustered into L clusters C_k for $0 \leq k \leq L - 1$ based on context-adaptive approach.
- Then reshape the predicted errors in each C_k into 2-D block having four columns and $\lceil |C_k| / 4 \rceil$ rows, the number of prediction errors is predicted by C_k .
- Then the two key-driven cyclical shift operations i.e., column shift and row shift are performed and read the data in raster-scan order to obtain the permuted cluster.

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

- The assembler adds the permuted clusters to form the final encrypted image that is then being passed to Charlie with the length of each cluster.

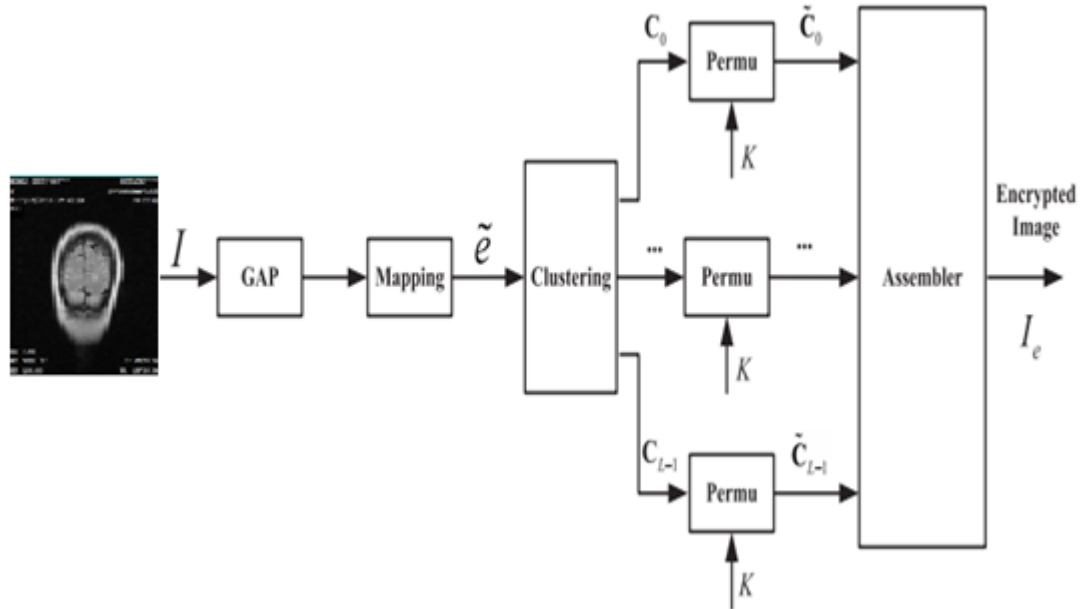


Fig. 1.5 Schematic diagram of image encryption

1.3.2 GAP (Gradient Adjusted Predictor)

Predictor uses local gradient estimation and three heuristic defined thresholds to detect edges

$$g_v = |W - WW| + |N - NW| + |N - NE|$$

$$g_h = |W - NW| + |N - NN| + |NE - NNE|$$

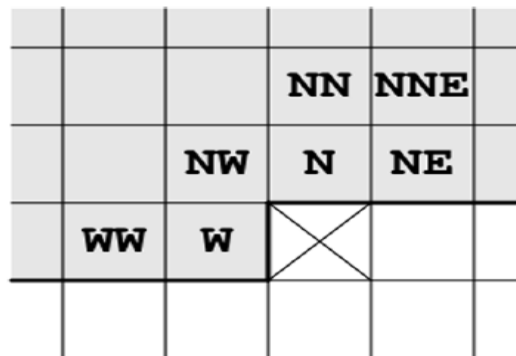


Fig.1.6 Gradient Adjusted Predictor

$$\begin{aligned}
 & \text{if } g_v - g_h > 80, P=W \\
 & \text{elseif } g_v - g_h < -80, P=N \\
 & \text{else } P = (W + N)/2 + (NE - NW) / 4 \\
 & \text{if } g_v - g_h > 32, P = (P + W) / 2 \\
 & \text{elseif } g_v - g_h > 8, (3P + W) / 4 \\
 & \text{elseif } g_v - g_h < -32, P = (P + N) / 2 \\
 & \text{elseif } g_v - g_h < -8, P = (3P + N) / 4
 \end{aligned}$$

1.3.2.1 Key features of GAP

- MED is exceptionally basic and productive indicator that perceives three separate sorts of causal regions
- GAP utilizes gradient estimation and edges for prediction
- Proposed Gradient Edge Detection
- Similarly to GAP, local gradient is estimated, but unlike GAP, proposed solution uses only one threshold, which can be user defined.

1.3.3 Column and Row Shift Operations

CS_k and RS_k be the secret key vectors controlling the row and the column movement balances for C_k . Here, C_k and RS_k are gotten from the key stream created by a stream figure, which suggests that the utilized key vectors could be diverse, notwithstanding for the same picture encoded at distinctive sessions. The irregular change is additionally shown in Fig. for an information arrangement $S = s_1s_2\dots s_{16}$, where the numbers inside the squares signify the lists of the components of S . Before doing permutations, the first column becomes (1,2,3,4), the second column turns into (5,6,7,8), and so on. The section movements are indicated by a key vector $CS=[3210]$, with every section experiencing a descending patterned move as per the key quality connected with that segment [6]. The technique is then repeated utilizing another key vector $RS=[2312]$ for each of the columns. Note that such change operations can be acknowledged by means of circular movements, which are effectively implemented in either software or hardware.

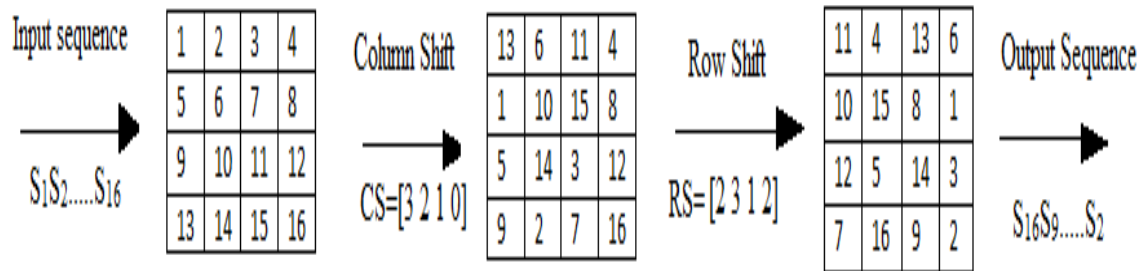


Fig. 1.7 An example of cyclical shift

1.4 Image Compression

Image compression addresses the problem of reducing the amount of data required to represent a digital image that intended to yield a compact representation of an image which reducing the image storage/transmission requirements. Compression achieved by the removal of one or more of the three basic data redundancies:

- Coding Redundancy
- Interpixel Redundancy
- Psychovisual Redundancy

Coding redundancy is available when not exactly optimal codes words are utilized and correlations between the pixels of a image are used by interpixel redundancy to conduct results. Due to information redundancy of psychovisual that is overlooked by the human visual framework, the image compression methods are used which decreases the quantity of bits which needed to represent a image by exploiting these redundancies where the backwards process called decompression (disentangling) where it is connected to the packed information to get the recovered picture.

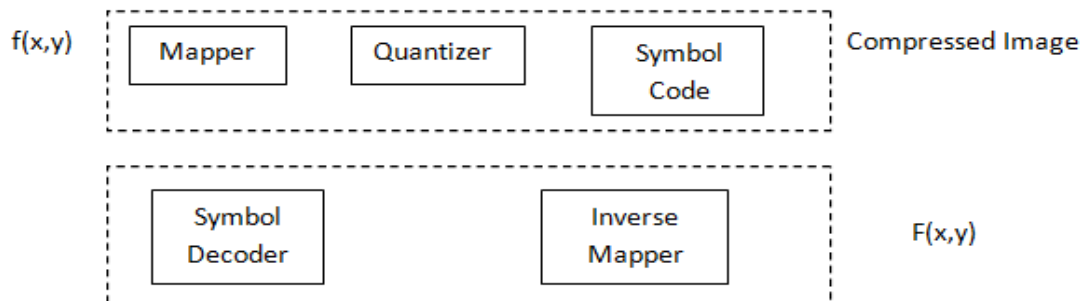


Fig. 1.8 Block Diagram of Image Compression

Encryption-then-Compression System using Haar and Symlet Wavelet Transform


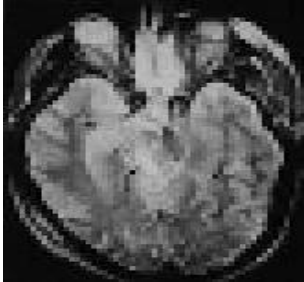

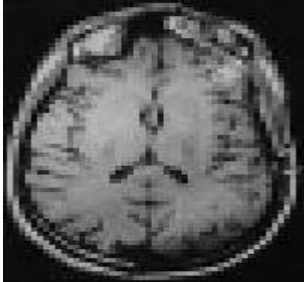

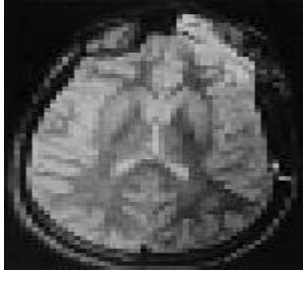
Image	Original Image	Compressed Image
synpic2712		
synpic2691		
synpic2692		

Table 1.2 Lists of Compressed Images

1.4.1 Wavelet Transform

One-dimensional wavelet theory defines a function Ψ , the wavelet, and its associated scaling function Φ , such that the family of functions $\{\Psi_j(x)\}; j \in \mathbb{Z}$, where $\Psi_j(x) = \sqrt{2^{-j}} \Psi(2^{-j}x)$, are orthonormal.

The continuous wavelet transform is defined by eq. 1.

$$C(a, b; f(t), \psi(t)) = \int_{-\infty}^{\infty} f(t) \frac{1}{\sqrt{a}} \psi^* \left(\frac{t-b}{a} \right) dt \dots \quad (1)$$

1.4.1.1 Haar Wavelet

The Haar transform is the simple and the basic transformations to a local frequency domain from the time/space domain, which shows the time/space variant spectrum. The characteristics of the Haar Transform are the speed at the time of implementation; establish it as potential candidate in developed computer engineering and electrical applications, like image and signal compression, capability to investigate the local characteristics. The Haar function is considered in the Haar transform, The Haar function is an Orthonormal, rectangular pairs. While the comparison of the Fourier transform basis function takes place, the difference between them is frequency. The Haar function changes in both the position and scale. The Haar transform is very nearly similar to the discrete Haar wavelet transform.

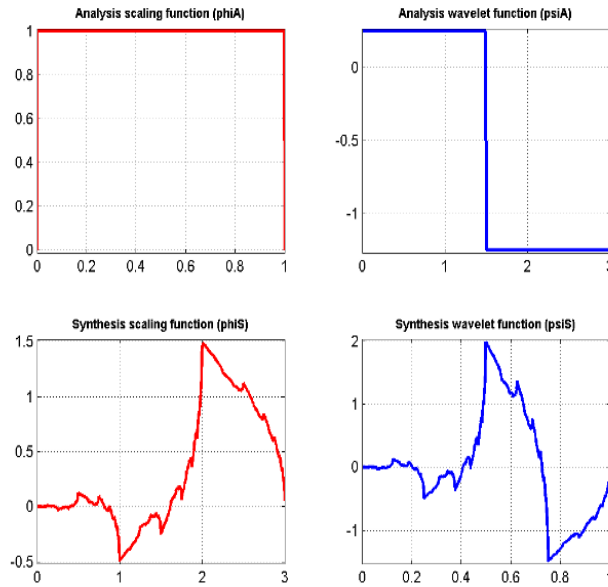


Fig. 1.9 Haar Wavelets

1.4.1.2 The Haar Function

At the interval $0 \leq t \leq 1$, The N Haar functions $h_k(t)$ are defined. The parameters p and q are used to determined the shape of the Haar function, i.e.,

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

$$k=2^p + q - 1 \quad \dots\dots(2)$$

where the range of k is within $k = 0,1,2,\dots,N - 1$.

The Haar function is considered as constant

when $k = 0$,

$$h_0(t) = 1/\sqrt{N} \quad \dots\dots(3)$$

when $k > 0$,

$$h_k(t) = \frac{1}{\sqrt{N}} \begin{cases} 2^{\frac{p}{2}} & \frac{q-1}{2^p} \leq t \leq \frac{q-0.5}{2^p} \\ -2^{\frac{p}{2}} & \frac{q-0.5}{2^p} \leq t \leq \frac{q}{2^p} \\ 0 & \text{otherwise} \end{cases} \quad \dots\dots(4)$$

It is examined from the above equation, the parameters p and q determines the width of that part of function which is non-zero and the p determines the amplitude.

The Haar matrix H formed by the discrete Haar functions is

$$H_{2N} = \begin{bmatrix} H_N & \otimes [1,1] \\ I_N & \otimes [1,1] \end{bmatrix} \quad \dots\dots (5)$$

$$H(0) = 1 \quad \dots\dots (6)$$

Where

$$I_N = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} \quad \dots\dots (7)$$

Where I_N is the identity matrix and \otimes is the Kronecker product. $A \otimes B$ is the Kronecker product where A is an $m \times n$ matrix and B is $p \times q$ is defined as

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \dots\dots(8)$$

When $N = 2^k$

$$H_N = \begin{bmatrix} \phi \\ h_{0,0} \\ h_{1,0} \\ h_{1,1} \\ \vdots \\ h_{k-1,0} \\ h_{k-1,1} \\ \vdots \\ h_{k-1,2^{k-1}-1} \end{bmatrix} \dots\dots(9)$$

where $I [1 \ 1 \ 1 \ \dots \ 1]$ is a $1 \times N$ matrix, and $h_{pq}[n]$ is a Haar function.

1.4.1.3 Symlet Wavelet

Symlet wavelets are a family of wavelets. Symlet wavelets are obtained by modifying the Daubechies by increasing their symmetry and retaining greater simplicity. They are orthogonal near symmetric and least asymmetry. They possess nearly the same characteristics as the db wavelets. In Matlab, it is used as symN, N is the order. They are an altered variant of Daubechies wavelets with expanded symmetry. Symlets are additionally orthogonal and minimally supported wavelets, which are proposed by I. Daubechies as a drug to the db family. Symlets are close symmetric also, have the minimum asymmetry. The related scaling channels are close straight stage channels. The properties of Symlets are about the same as those of the db wavelets.

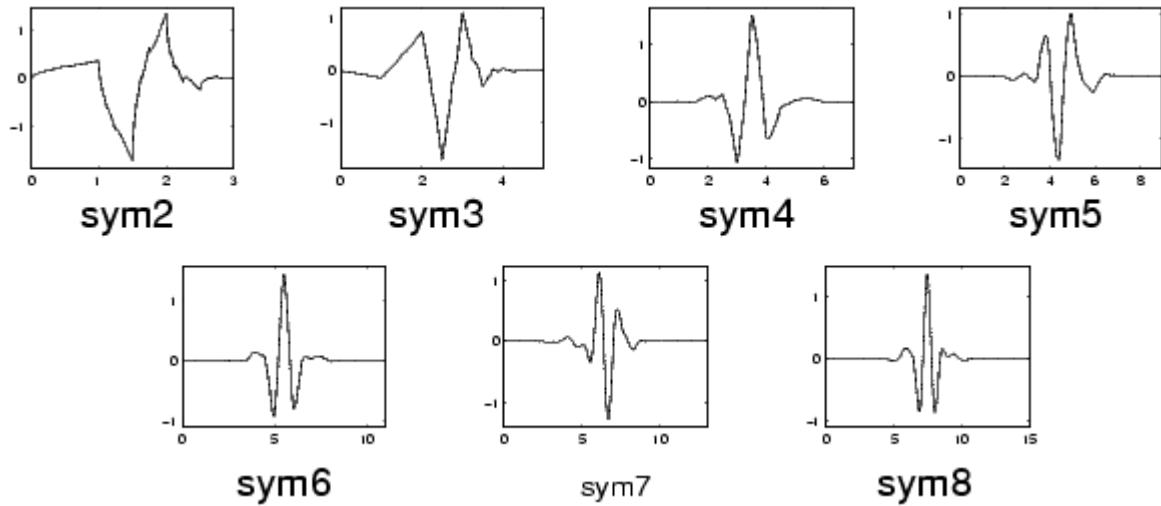


Fig.1.10 Symlet Functions

1.5. Evaluation Parameters

1.5.1. Compression Ratio (CR): The compression ratio i.e. the size of the compressed image is compared to that of the uncompressed image. Still images are often losslessly compressed at 10:1, but the quality loss is more noticeable, especially on closer inspection.

$$C_R = n_1 / n_2 \quad \dots\dots (10)$$

where n_1 is the size of original image and n_2 is the size of compressed image.

1.5.2. Mean Squared Error (MSE)

Mean Squared Error is basically a signal constancy measure. The objective of signal constancy, measure is to think about two signals by giving a quantitative score that depicts the level of closeness or, the level of blunder/error in the middle of them and on the other hand,. More often than not, it accept that one of the signal is an immaculate unique, while the other one is distorted by mistakes. The mean square error (MSE) between the signals is given by the accompanying equation:

$$MSE = (1/N) \sum |x(i) - e(i)|^2 \quad \dots\dots (11)$$

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

1.5.3. Peak Signal to Noise Ratio (PSNR)

Implanting or compressing additional information must not corrupt human impression of an object. Assessment of insensible is normally in view of a target measure of value, called Peak Signal to Noise Ratio (PSNR), or a subjective test with indicated strategies. The PSNR values can be gotten utilizing following equation:

$$\text{PSNR} = 20\log_{10} (\text{PIXEL_VALUE}/\sqrt{\text{MSE}}) \quad \dots\dots\dots (12)$$

1.5.4. Solidity

Scalar indicating the extent of the pixels in the arched body that are likewise in the region figured as Area/Convex Area. This property is upheld just for 2-D data name networks. The proportion of the object range to the curved area is known as the solidity/robustness. In the event that solidity of image is more than specific limit esteem then the nature of image has not been influenced because of compression.

1.5.5. Bit Error Rate

In advanced digital transmission, the quantity of bit errors is the quantity of received bits of an information stream over a communication channel that has been changed because of clamor/noise, interference, contortion or bit synchronization errors.

The bit error rate (BER) is the quantity of bit errors every unit time. The bit error rate (additionally BER) is the quantity of bit blunders separated by the aggregate number of exchanged bits at the examined time interval. BER is a unitless performance measure, regularly expressed as a percentage [1].

CHAPTER 2

REVIEW OF LITERATURE

Jiantao Zhou et.al [1] proposed designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation. For the security issues, image encryption has been implemented before the image compression. A highly efficient image Encryption- then- Compression (ETC) method is used where the compression used to compress the image is both lossless and lossy. The error prediction method is used to encrypt the image.

S. Dharanidharan et.al [2] proposed Modified International Data Encryption Algorithm using in Image Compression Techniques. Images can be encrypted in many ways; several techniques have used different encryption methods. In this research, they applied a new modified International Data Encryption Algorithm to encrypt the whole image in an efficient and secure way, the file will be segmented and converted to another image files after encryption.

R. Loganathan et.al [3] proposed on Active Contour Based Medical Image Segmentation and Compression Using Biorthogonal Wavelet and Embedded Zerotree. Medical image compression is required to reduce the storage of medical database which is done by any of the compression technique. One of the Region of Interest based approach i.e., active contour is used to **segment** the image into diseased part and the background [6]. The methods proposed have the expressive the results by improving the Peak Signal to Noise Ratio.

D.Maheswari et.al [4] proposed on Improved Block Based Segmentation and Compression Techniques for Compound images. The main task of image compression is to reduce the size of image or any graphics file in bytes while unaffected the quality of the image. Generally, there are three classification methods that is used to compress the compound image i.e., layer based, block based and object based. The block based classification is enhanced with two techniques AC-Coefficient Based Model and Histogram based model. It is evaluated that the

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

histogram based segmentation method has better compression ratio and lesser compression and decompression time as compared with AC-Coefficient method.

R.Janaki et.al [5] proposed on Enhanced Lossy Techniques for Compressing Background Region of Medical Images Using ROI-Based Encoding [1]. The Region of interest based methods uses both the compression i.e., lossless and lossy. The enhanced ROI technique is used to segment the image which is active contour. JPEG algorithm is used to compress the image. The proposed technique gave better results on the basis of Peak Signal to Noise Ratio as well as compression speed than the previous traditional techniques.

Ch. Samsu et.al [6] proposed on An RGB Image Encryption Supported by Wavelet-based Lossless Compression. In this paper he proposed a method for an RGB image encryption supported by lifting scheme based lossless compression. A 2-D integer wavelet transform and lossless predictive coding is used to sequentially to compress the input color image, the compressed image was then encrypted by using Secure Advanced Hill Cipher (SAHC) involving a pair of involutory matrices, a function called Mix () and XOR. It is conducted that there is no difference between the input and the output image after decryption. The proposed method can be used for efficient and secure transmission of image data.

M. Firoozbakht et.al [7] proposed Compression of digital medical images based on multiple regions of interest. In order to reduce the storage cost and transmission time, a context-based and regions of interest based approach is implemented to compress the images. The image is segmented into the 3 parts defining as primary region of interest, secondary region of interest and the background where the primary region of interest is identified manually. An in house 3D region growing algorithm is used to recognize the secondary regions of interest with the help of primary region of interest. By using this methodology, the image is compressed in such a efficient way that size is reduced up to 67 percent.

R. Janaki et.al [8] proposed on Enhanced ROI (Region of Interest Algorithms) for Medical Image Compression. ROI based techniques are extensively used as there are some regions in the medical image which demands high quality. A ROI based approach is used to segment the image into foreground image and the background region. The techniques are Mixed

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

Raster Layering, Region Growing and the active contours which are enhanced to segment the image into interested and non interested region. The active contour and the region growing technique are effective and efficient than the other two techniques.

Guiliang Zhu et.al [9] presented a Digital image encryption algorithm based on pixels in which their algorithm possesses security at high level and huge key space where there needs a high security of interactive information in various areas like national security, military, aerospace etc.

Ma, K. et.al [10] presented Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption. They maintains the feature where the original cover can be recovered losslessly after implanted information is extracted as well as preserving the confidentiality of the content of the image. The method can achieve that the image the y recovered and the data that are extracted are free from error.

Ravishankar K. C. et.al [11] proposed Region based selective image encryption where they used many methods to encrypt the image and by using that method, the content is not visible as their methods develop randomness in the image. They achieved high efficiency and various other advantages over the previous methods.

Jiantao Zhou et.al [12] presented on the design of an encryption-then-compression system. They presented permutation-based image encryption scheme where they design arithmetic coding technique to compress the image and the performance of compression is closed to the compression performance of the unencrypted original image having slight degradation in performance.

Bianchi, T. et.al [13] presented work on the Implementation of the Discrete Fourier Transform in the Encrypted Domain where the implementation of the Discrete Fourier Transform is investigated by utilizing the homomorphic properties of the underlying cryptosystem in the encrypted domain. They demonstrated that radix-4 fast transform is the best one for the encrypted domain in their proposed scenario.

R. Mehala et.al [14] proposed a new image compression algorithm using Haar Wavelet Transformation. In that paper, by putting some 0's and $\frac{1}{2}$'s into the Haar Wavelet, 8X8

transform matrix can be evaluated. The premise of the Haar Wavelet calculation was in view of numbers, and made sufficiently inadequate orthogonal transform matrix and developed A Haar Wavelet algorithm for fast processing.

X. Zhang et.al [15] proposed compression of encrypted images with multilayer decomposition. That work proposed a plan of Lossy Compression for encoded gray images. In the encryption stage, the given image was decayed into sub-image and the few layers of predicted errors, and they were encoded utilizing a selective or operation and pseudo-random permutation. As channel supplier did not know the cryptographic key and the original data, at collector side with the learning of cryptographic key, a decoder incorporating dequantization, decryption and picture remaking functions were utilized to recover the essential substance of original image from the compressed information.

J. Zhou et.al [16] proposed l2 reclamation of l_∞ -decoded images by means of delicate choice estimation. The new delicate interpreting methodology was produced to diminish the l2 distortion of l_∞ -decoded images and hold the preferences of both min-max and least square rough guesses. The new delicate interpreting strategy had the capacity even outperform JPEG 2000 for bit rates higher than 1bpp, a basic rate district for utilizations of close lossless image compression. All the coding additions were made without expanding the encoder unpredictability as the large calculations to increase coding efficiency were appointed to the decoder.

D. Kline et.al [17] investigated compression of data encrypted with block ciphers, such as the Advanced Encryption Standard. It was shown that such data was able to be feasibly compressed without knowledge of the secret key. Block ciphers operated in various chaining modes were considered and it was shown how compression was to be achieved without compromising security of the encryption scheme. Further, it was shown that there existed a fundamental limitation to the practical compressibility of block ciphers when no chaining was used between blocks.

Z. Erkin et.al [18] generated private recommendations efficiently using homomorphic encryption and data packing. By presenting a semi-trusted outsider and utilizing data

packing, they build an exceedingly efficient framework that did not require the dynamic cooperation of the user. They additionally displayed a comparison protocol, which was the first to the best of their insight that compare about different values that were pressed in one encryption.

A. Kumar et.al [19] proposed Lossy compression of encrypted image by compressing sensing technique. A method was proposed to attain the compression of the encoded image information based on compressive sensing technique. Joint decoding/decryption were proposed with the modified basis pursuit decoding method to handle the encryption.

Miss S.S. Tamboli et.al [20] proposed Image Compression using Haar Wavelet Transform. In that paper, Haar Wavelet Transform was conducted. The outcomes regarding PSNR and MSE demonstrate that the Haar wavelets had the capacity to be utilized for image compression. The quantization was finished by isolating the picture matrix into squares and taking mean of the pixel in the given square. It was clear that DWT had potential application in the compression issue.

X. Zhang et.al [21] proposed Compressing encrypted image using compressive sensing. The original image was encoded as a set of coefficients by a secret orthogonal transform. Since the image had inadequate representation in conventional transform space and had the capacity to be recuperated from a little amount of measurements, the encoded picture information was compressed into a progression of measured information. Utilizing signal recovery system for compressive sensing, a recipient had the capacity to remake the content of original image.

M. Barni et.al [22] proposed Privacy-preserving ECG classification with branching programs and neural networks. That paper focused on the development of a privacy preserving automatic diagnosis system whereby a remote server classifies a biomedical signal provided by the client without getting any information about the signal itself and the final result of the classification. Specifically, they present and compare two methods for the secure classification of ECG signals: the former based on linear branching programs and the latter relying on neural networks. The paper deal with all

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

the requirements and difficulties related to working with data that must stay encrypted during all the computation steps.

Asha P. Ghodake et.al [23] proposed Modified Scheme for Lossy compression and iterative reconstruction for encrypted image. A pseudo-random permutation was utilized to scramble an original image, and the encoded information was effectively compressed via disposing of the unreasonably harsh and fine data of coefficients created from orthogonal change. In the wake of getting the compressed information, with the help of spatial correlation in regular picture, a beneficiary had the capacity reproduce the primary substance of the original image by iteratively updating the values of coefficients.

W. Liu et.al [24] proposed Efficient compression of encrypted grayscale images. Lossless compression of scrambled sources had the capacity to be attained through Slepian-Wolf coding. They proposed a resolution dynamic compression method where the encoded image is compressed in resolution such decoder notices the image in low resolution and study the local statistics based on it and utilize the measurements to decode the upcoming resolution level.

T. Bianchi et.al [25] proposed Composite signal representation for fast and storage-efficient processing of encrypted signals. The proposed representation permitted users to decrease the size of encoded signals and to speed up linear operations on encoded signals by parallel processing. They presented the merits of the proposed representation and give some insights regarding the signal processing algorithms that are more reliable to work on the composite representation by a case study 1-D linear filtering.

V. Ashok et.al [26] proposed The Fast Haar Wavelet Transform for Signal & Image Processing. A method for the design of Fast Haar wavelet for signal processing & image processing had proposed. The analysis bank and synthesis bank of Haar wavelet was modified by using polyphase structure. Finally, the Fast Haar wavelet was designed and it satisfied alias free and perfect reconstruction condition. Computational time and computational complexity was reduced in Fast Haar wavelet transform.

Q. M. Yao et.al [27] proposed Multi-resolution based hybrid spatiotemporal compression of

encrypted videos. That paper proposed a novel multi-resolution based approach which made it possible not only to effectively derive the temporal side information from previous frames, but also to generate the spatial side information by having partial access to the current frame. The spatial and temporal side information was able to then be integrated adaptively to facilitate the compression.

T. Bianchi et.al [28] proposed on the implementation of the discrete Fourier transform in the encrypted domain by using the homomorphic properties of the underlying cryptosystem. Various kinds of issues are determined for the direct DFT: the radix-2 and the radix-4 fast Fourier algorithms, including the analysis of error and the maximum size sequence that can be transformed.

A. Kumar et.al [29] proposed Lossy compression of encrypted image by compressing sensing technique. A method was proposed to attain the compression of the encoded image information based on compressive sensing technique. Joint decoding/decryption were proposed with the modified basis pursuit decoding method to handle the encryption.

T. Bianchi et.al [30] proposed Encrypted domain DCT based on homo-morphic cryptosystems. A 1-dimensional DCT was conducted by defining a convenient signal model and by utilizing the separable processing of rows and columns; 1-d was extended to the 2-dimensional case. The bounds of cryptographic system on the size of the DCT and the arithmetic precision were derived, considering both the direct DCT algorithm and its fast version. The application of the s.p.e.d. 2D-DCT and 2D-BDCT to 8-bit grey-scale images was analyzed; whereas it is demonstrated the feasibility of s.p.e.d DCT in real scenario by the case study.

D. Schonberg et.al [31] proposed toward compression of encrypted images and video sequences. They first created statistical models for images before stretching out it to videos, where their procedures truly pick up traction. The recent compresses every decoded frame of the "Foreman" test succession by 59% of average. In examination, their confirmation of-idea execution, working on encoded information, compresses the same

sequence by 33%. Next, they create and present an adaptive protocol for widespread compression and demonstrate that it converges to the entropy rate.

R. Lazzeretti et.al [32] proposed Lossless compression of encrypted grey-level and color images. In that paper they research the possibility of encoded gray level and color images, by disintegrating them into bit-planes. A couple of ways to deal with endeavor the spatial and cross-plane correlation among pixels were talked about, and additionally the possibility of misusing the correlation between color bands.

A. Kumar et.al [33] proposed Distributed source coding based encryption and lossless compression of gray scale and color images. In this paper, they considered the encryption, which is then followed by lossless compression of gray scale and color images. The proposed encryption is based on the prediction errors instead of directly applying compression on the images and use distributed source coding for compressing the encoded texts.

D. Schonberg et.al [34] proposed on compression of encrypted images. In this work, they use a 2-D source model, and create method to compress encoded images based on LDPC codes. They presented practical simulation results for compressing bi-level images. In tests, they were attained the capacity to compress an encrypted 10, 000 bit bi-level image to 4, 299 bits and are able to recover the original image successfully whereas in previous researches, the analogous 1-D model (that is operating on a raster scanned data sequence of the same source) could only compress the image to 7, 710 bits.

D. Schonberg et.al [35] proposed on blind compression of encrypted correlated data approaching the source entropy rate. They proposed and analyzed an incremental method that is based on exponentially increasing block lengths which was created to balance the resolution rate of parameter estimate with the redundancy rate of communication and also show that the redundancy at best declines is proportional to the inverse of the square root of the block length by implementing the ideas based low-density parity check (LDPC) codes.

K. Wahid et.al [36] proposed on Error-free computation of 8×8 2D DCT and IDCT using two-dimensional algebraic integer quantization. The architecture used a new algebraic integer quantization of a 1D radix-8 DCT that allowed the

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

separable computation of a 2D 8×8 DCT without any intermediate number representation conversions. Using this encoding scheme, an entire 8×8 1D DCT-SQ (scalar quantization) algorithm was able to be implemented with only 24 adders.

M. Johnson et.al [37] proposed on compressing encrypted data. In the work, they researches the novelty of reversing the order of these steps, i.e., first encrypting that is followed by compressing, without compromising information security and the efficiency of compression. Although counter-intuitive, they show that, through the use of coding with side information principles, without losing both secrecy and target coding efficiency, this reversal of order was indeed possible in some settings of interest.

Piotr Porwik et.al [38] proposed The Haar Wavelet Transform in Digital Image Processing: Its Status and Achievements. In this paper, it was displayed that two-dimensional both, the Haar and wavelets capacities items may be dealt with as extractors of specific image highlights. Moreover, it was additionally demonstrated that a few coefficients from both spectra were relative, which simplify slightly calculations and investigations.

Bryan Usevitch [39] proposed A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000. One of the reasons of this article was to give a general gathering of people sufficient background into the details and procedures of wavelet coding to better comprehend the JPEG 2000 standard. The attention was on the key standards of wavelet coding and not the real standard itself. There were two sorts of filter choices: orthogonal and bi-orthogonal. Orthogonal channels had the property that there was energy or norm preserving and the modern wavelet coders use bi-orthogonal filters which did not protect energy. Other modern wavelet coders that broaden the thoughts found in the EZW calculation were also described.0and analyses.

Haweel T.I. [40] proposed a new square wave transform based on the DCT. An efficient SWT was exhibited. It was based on applying the signum function operator to the conventional DCT and was termed the marked DCT/SDCT. No request limits were forced on the measurements of the SDCT. Quick forward and in reverse transformations may be attained to. No increase operations or transcendal expressions were needed. Investigation and

simulations were acquainted with demonstrate that the proposed SDCT kept up the great de-correlation and power compaction properties of the DCT.

M. J. Weinberger [41] proposed The LOCO-I loss-less image compression algorithm: Principles and standardization into JPEG-LS. LOCO-I was the algorithm at the core of the new ISO/ITU standard for lossless and near-lossless compression of continuous-

tone images, JPEG-LS. By combining simplicity with the compression potential of context models, the algorithm “enjoys the best of both worlds”. The proposed model has the capability for capturing the high-order dependencies of the more complicated wide techniques.

X. Wu et.al [42] proposed Context-based, adaptive, lossless image codec. In this learning process, the CALIC evaluated only the desire of expectation errors considered on countless contexts as opposed to evaluating an expansive number of conditional probabilities. The previous estimation method had the capacity bear the cost of countless modeling contexts without suffering from the context dilution issue of lacking of counting statistics as the last approach, not from intemperate memory utilization. The low time and space complexities were additionally credited to efficient methods forming and quantizing demonstrating settings.

A. J. Menezes et.al [43] published Handbook of Applied Cryptography. In this work, there are two essential objectives inspired by the "handbook" nature that is to permit simple access to remain solitary results, and to permit results and calculations to be effectively referenced. To encourage the ease of access and reference results, things had been ordered and numbered to a vast degree, with the accompanying classes of things together numbered successively in every part: Definitions, Examples, Facts, Notes, Remarks, Algorithms, Protocols, and Mechanisms. In more conventional medicines, Facts were generally recognized as suggestions, lemmas, or theorems. They utilized numbered Notes for extra specialized focuses, while numbered Remarks distinguish non-specialized remarks, observations and opinions.

CHAPTER 3

PRESENT WORK

3.1 Objectives

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

- To reduce the storage cost, diagnostic analysis cost and transmission time without significant reduction of the image quality by using the enhanced image compression technique.
- To provide the secure transmission of the medical images, encryption of the medical images is conducted before compression which helps to face the security risks at the transmission of the medical images.
- The accuracy of the compressed image after the transmission of the image to the client is measured. Effective techniques are to be developed to decrease the effect of compression on the image.
- 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.
- 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 SYMLET wavelet.

3.2 Formulation of problem

In numerous useful situations, image encryption must be directed before image compression. This has prompted issue of how to plan a couple of image encryption and compression such that compression of encoded images can in any case be proficiently performed. The image encryption method was worked with random permutation technique which still has the capacity to provide high state of security. To compress the encoded image a arithmetic coding based approach was exploited. The compression approach applied to the encrypted image is only slightly worse in terms of compression efficiency. Increasing compression efficiency of the encrypted image, a new Image compression algorithm using Haar and Symlet Wavelet Transform is implemented on the encrypted image. The basic of the proposed Haar and Symlet Wavelet algorithm is based on the integers and made sufficiently sparse orthogonal transform matrix. The proposed 8X8 transform matrix can be obtained by appropriately inserting some 0's and $\frac{1}{2}$'s in to the Haar and Symlet Wavelet. This proposed methodology has been implemented in MATLAB. Proposed technique results are compared to the previous work using various evaluation parameters like Compression-Ratio, MSE and PSNR. Techniques and parameters were mentioned above. Now, say this proposed technique as ECNHWT (Encryption-Compression using new Haar and Symlet Wavelet Transform). This is called as new Haar and Symlet Wavelet Transform because we are implementing Haar and Symlet Wavelet Transform for image compression using a new algorithm which was proposed by R. Mehala .The formulation of problem that is mentioned above can be concluded in following steps:

- Many Image Compression procedures used to compress the encoded image have been proposed before yet they were not sufficiently secure and compression ratio was not very great.
- Image Compression couldn't give better results as strategy utilized for Compression with context based arithmetic coding was sufficiently bad. That is the reason we are utilizing another image encryption algorithm of Haar and Symlet Wavelet Transform.
- Results are assessed utilizing different parameters like CR, MSE and PSNR

3.3 Work Methodology

In this work, a novel approach for image encryption and compression is used in which random permutation method is combined with new Haar and Symlet Wavelet Transform for calculating more accurate results. The proposed approach is named as ECNHWT (Encryption-Compression using new Haar and Symlet wavelet transform).

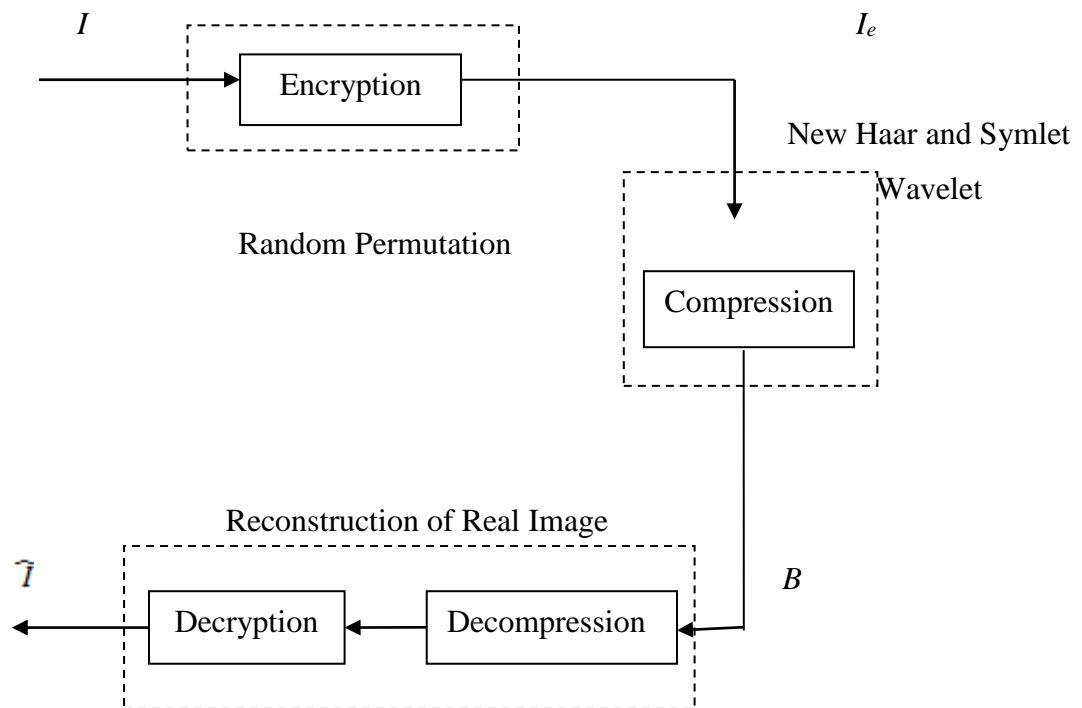


Fig. 3.1 Proposed Model for Encryption-Compression System

3.3.1 Encryption-Compression using new Haar and Symlet wavelet transform (ECNHWTNS)

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 and Symlet 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.

As shown in Fig. 3.1 Encryption-Compression system is proposed. The resultant image \hat{I} is evaluated using various parameters like CR, MSE and PSNR to check the efficiency and to

compare it with the result of existing system. Also represent the proposed schema with the help of flowchart. Fig. 3.2 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.

3.3.2 Procedure for algorithm performing the image encryption-compression by new Haar and Symlet wavelet transform (ECNHWTNS) is given as follows [7]:

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 C_k , for $0 \leq k \leq L - 1$, and each C_k is formed by concatenating the mapped prediction errors in a raster-scan order.
- III: Reshape the prediction errors in each C_k into a 2-D block having four columns and $\lceil |C_k| / 4 \rceil$ rows, where $|C_k|$ denotes the number of prediction errors in C_k .
- 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 $0 \leq k \leq L - 1$, and generates the final encrypted image $I_e = \tilde{C}_0 \tilde{C}_1 \dots \tilde{C}_{L-1}$ 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 I_e together with the length of each cluster $|\tilde{C}_k|$, for $0 \leq k \leq L - 1$.

Step 2: Implementation of compression algorithm to the outcome of above algorithm

i.e. I_e

- I. Treat the array as $n/2$ pairs called (a, b)
- II. Calculate $(a + b) / \sqrt{2}$ for each pair, values becomes first half of the output array.
- III. Calculate $(a - b) / \sqrt{2}$ for each pair, values become 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 $\frac{1}{2}$'s into the HWT.

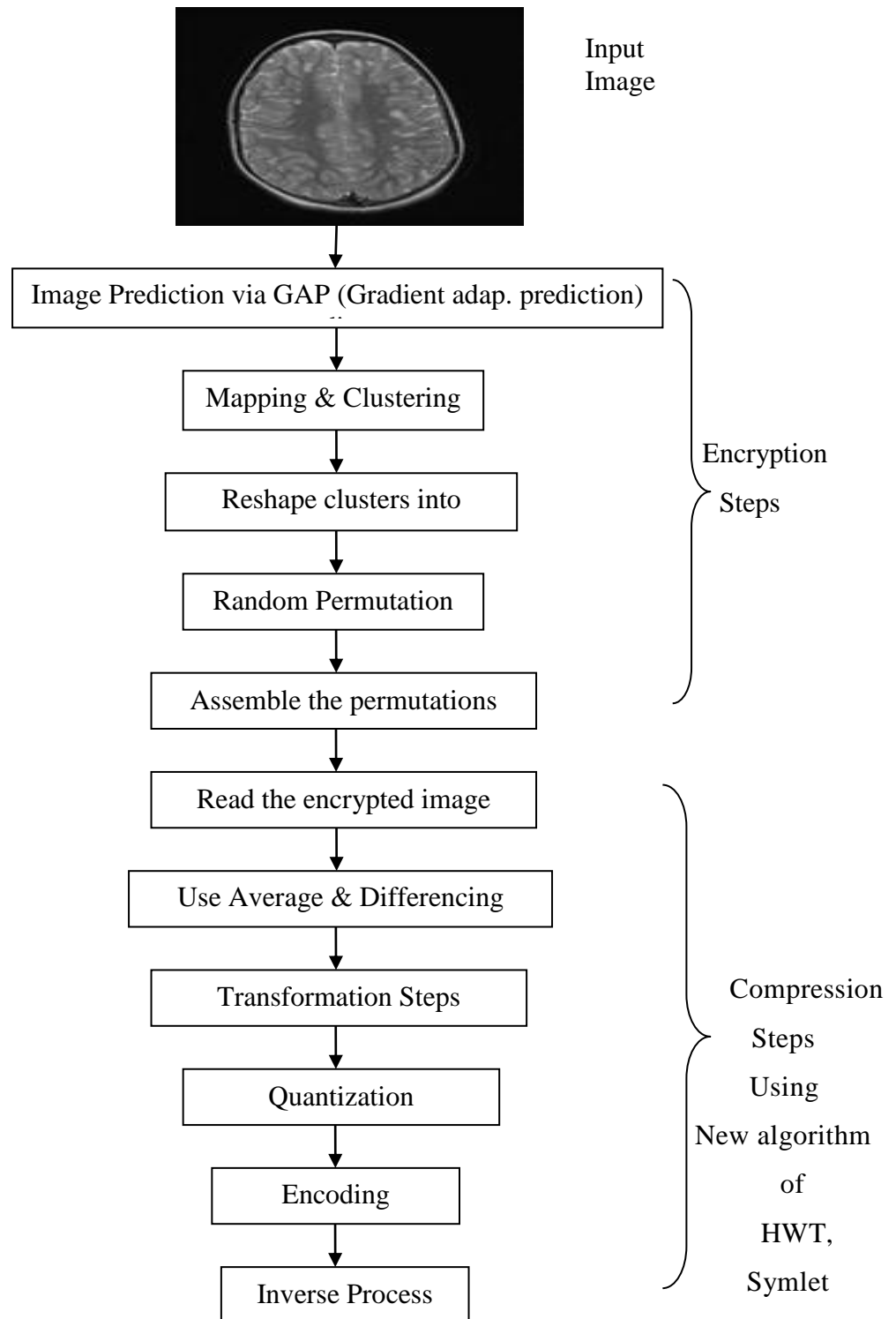


Fig. 3.2 Flowchart for Image Encryption-Compression Scheme

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

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 before it can be obtained for multiplying on the right by the matrix.

Step 3: Applying the inverse 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.

In this new image compression algorithm of Haar and Symlet 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.

3.4 Software used

MATLAB defines the programming environment for development of algorithm, analysis of data, visualization, and numerical computation. MAT Lab stands for Matrix Laboratory, helps to solve the technical computing problems faster than with traditional programming language which are: C, C++ and Fortan. MAT Lab allows solving many technical computing problems and especially those with matrix and vector formulations. By using MATLAB in a wide range of an application which includes these all: signal and image processing, communication, control design, test and measurement, financial modeling & analysis, computational biology.

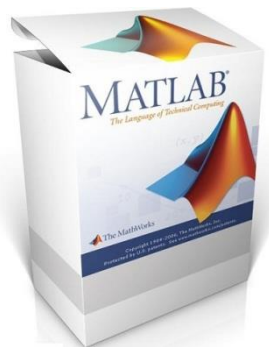


Fig. 3.3 Software used- MATLAB

Computing technical high performance language where integrates computation, visualization and also programming in an easy-to-use environment where it defines the problems and solutions are expressed in familiar mathematical notation also include Math and computation algorithm development Data acquisition Modeling, simulation and prototyping Data analysis, exploration, visualization Scientific and engineering graphics application development which including graphical user interface building.

3.4.1 The MATLAB System

The MATLAB have five parts:

- The MATLAB language: High-level grid, array language with control of calculations stream, data structures, capacity, info yield and object-oriented programming highlights. Both programming in the little to immediately make dirty throw-away programs and for programming in the vast is to make complete large and complex application programs.
- The MATLAB working environment: Set of instruments and offices work with MATLAB client or developer. Including facilities for controlling variables in workspace and importing and trading information. Including devices for creating, managing, debugging, profiling M-files and applications.
- Handle Graphics: This is also called MATLAB representation system which incorporates high-level commands for two-dimensional furthermore for three-dimensional with data of image processing, animation, visualization and presentation of graphics. Handle Graphics incorporates the low-level commands that permit you to completely modify the presence of graphics likewise to construct complete Graphical User Interfaces on MATLAB applications.
- The MATLAB mathematical function of library: This is also called the large collection of computational algorithms that are ranging from elementary functions like sum, sine, cosine, and complex arithmetic. Functions like, Bessel functions, eigen values, inverse matrix, fast Fourier transforms.
- The MATLAB with Application Program Interface (API): API is a library that permits to compose C and Fortran programs which help to associate with MATLAB furthermore incorporate facilities for calling routines from MATLAB (element connecting), calling MATLAB as a computational engine, and for perusing and composing MAT-files.

3.4.2 Image Processing Toolbox

The core MATLAB package accompanies a several rudimentary functions that can be utilized to load, save and perform custom functions on images. Often, it is perform to perform more complicated operations on images. The image processing toolbox allows:

- Images in MATLAB having direct visualization.
- Color space conversions.
- Object grouping and data collection.
- Filtering and fast convolution.
- Fourier analysis of images.
- Image arithmetic.
- Morphological operations.

3.4.3 Why MATLAB?

MATLAB is scientific programming language and provides strong mathematical and numerical support for the implementation of advanced algorithms for this reason MATLAB is widely used by the image processing and computer vision community. Algorithms were implemented first in MATLAB only be available in MATLAB.

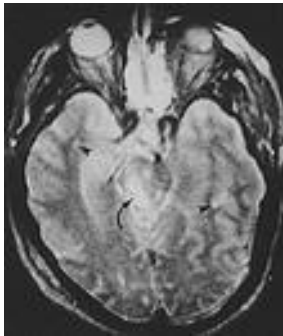
- It guarantees steps of image processing which utilized as totally documented and can be duplicated.
- The source code for all image processing function which available for scrutiny and test.
- Allowing one to guarantee numerical precision is maintained completely through the enhancement process.
- Image processing algorithms accessible in MATLAB to be best in class than those accessible from image processing applications.
- Development, research with high efficiency and analysis tools.
- Add-on application-specific solutions called toolboxes.
- Its workspace comprises of the sets of variables develop during a MATLAB session and stored in memory.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Results

The objective of the 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. 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 Haar and 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 CR (Compression Ratio), MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio).



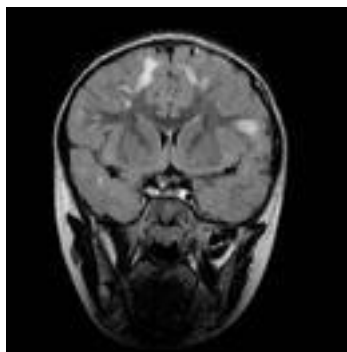
(a) synpic2712



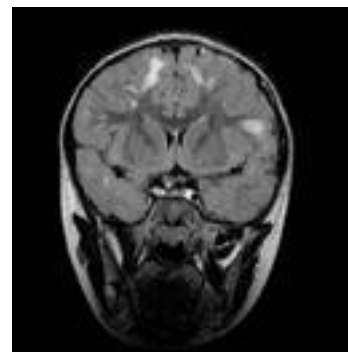
(b) synpic2691



(c) synpic2692



(d) synpic2693



(e) synpic12338

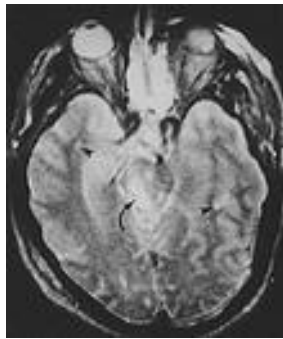
Encryption-then-Compression System using Haar and Symlet Wavelet Transform

Fig. 4.1 Grayscale Images (a) synpic2712 (b) synpic2691 (c) synpic2692 (d) synpic2693 (e) synpic12338

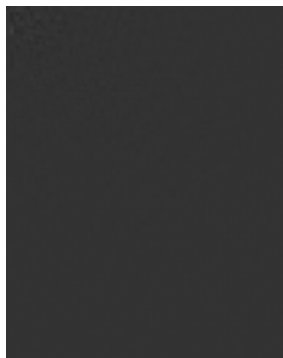
Any intruder trying to interfere in between the transmission will neither be able to alter, nor to copy the content. The proposed technique has been applied to grayscale images and gives satisfactory results. The techniques have been implemented on a set of 5 grayscale images of dimension 512x512 of jpeg extension. The performance of the proposed work has been evaluated and graphically represented on the basis of three measures: Compression-Ratio (CR), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

4.1.1 Encryption

For encryption any one of the given set from Fig 4.1 of grayscale images is taken. The synpic2691 is grayscale image



(a) synpic2712



(b) Encrypted Image Encrypted.jpg

Fig. 4.2 Encryption of synpic2712 (a)-(b)

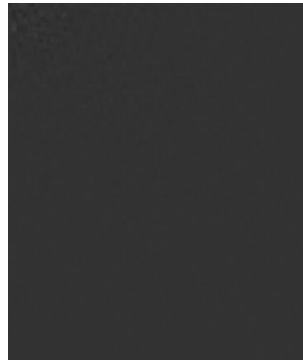
This process is done to encrypt the image that we need to send at some destination. In cover image synpic2712.jpg the pixels of image is in readable format means one can easily recognize the image so to convert it into unreadable format we apply random permutation

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

method on it and the output is as shown in Encrypted.jpg. The dimension of encrypted image remains same as that of cover image.

4.1.2 Compression

After the encryption of image, in this section encrypted image is transformed into compressed image. However the pixel size remains the same but there is change in storage size. For human eye there is no difference in outlook of these two images but there is lots of difference in their pixel values and storage size.



(a) Encrypted image Encrypted.jpg



(b) Compressed image Compressed.jpg

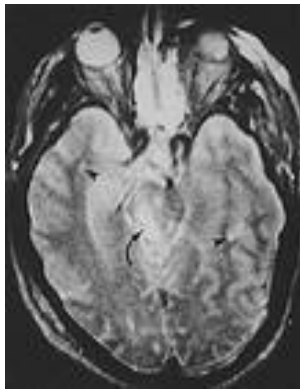
Fig. 4.3 Compression of Encrypted image (a)-(b)

4.1.3 Decompression & Decryption

Under this section the sequential decompression and decryption of the compressed image take place. Reconstruction of real image is done by using decompression & decryption algorithms respectively.



(a) Compressed image Compressed.jpg



(b) Reconstructed image Reconstructed.jpg

Fig. 4.4 Reconstruction of real image (a)-(b)

4.1.4 Key Steps of the Encryption then compression using Haar and Symlet Wavelet Transform

- Upload the image from the database.
- Filter the image to remove the noises if any
- Encrypt the image by random permutation
- Compress the image using Haar and Symlet Wavelet Transform

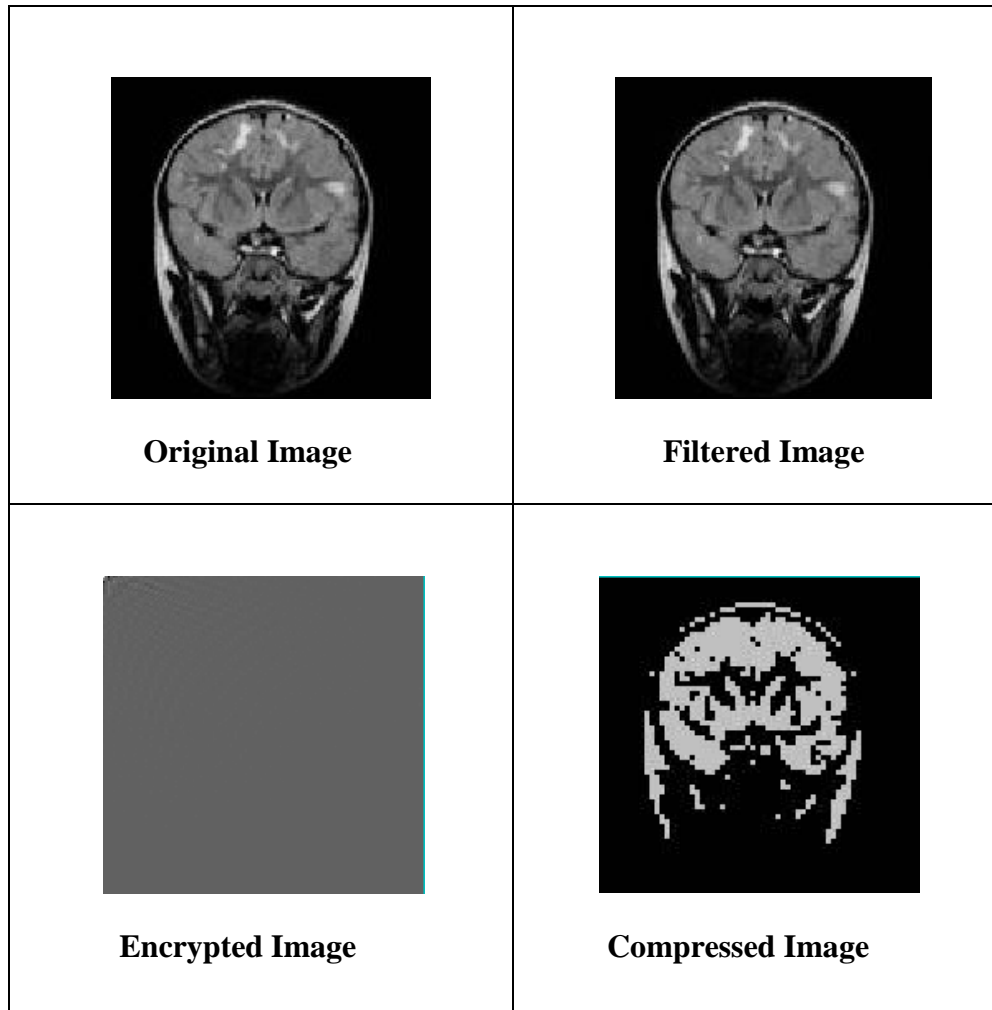


Table4.1 Layout of various resultant images

4.1.4 CR, MSE & PSNR Calculation for Performance Analysis

For the performance analysis images of synpic2712, synpic91, synpic92, synpic93 synpic12338 are considered as input images shown in Fig. 4.1. The CR, MSE and PSNR of different input images are shown in table 4.1 and table 4.2 shows the comparison of proposed work with the existing one.

The CR, MSE & PSNR is calculated for more than one image that's why the average value of CR, MSE & PSNR is also shown in table 4.2 and table 4.3 and the BER and Entropy and Entropy values are in Table 4.4 and Table 4.5.

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

S. No.	Image (.jpeg)	CR (Compression Ratio of previous work)	CR (Compression Ratio of proposed work)	MSE (Mean Square Error of proposed work)	PSNR (Peak Signal to Noise Ratio of proposed work)
1	sync2712	11.6224	12	1.9475	53.8599
2	sync2691	11.757	22	1.7309	56.0260
3	sync2692	11.5209	20	1.8533	54.7691
4	sync2693	11.6657	20	1.9240	54.0827
5	sync12338	9.73146	15	1.8092	59.1317
Average			17.8	1.85298	55.57388

Table 4.2 CR, MSE and PSNR

4.1.5 Comparison of PSNR, BER, Entropy for Existing method (ETC) & proposed method (ECNHWTNS)

The PSNR in the case of proposed method is more than the PSNR in existing method as shown in table 4.2. It means our proposed method (ECNHWTNS) gives better results as compared to existing method [1].

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

S. No.	Image (.jpeg)	CR (Compression Ratio of previous work)	CR (Compression Ratio of proposed work)	MSE (Mean Square Error of proposed work)	PSNR (Peak Signal to Noise Ratio of proposed work)
1	synpic42040	13.4816	22	1.6959	56.4032
2	synpic42042	10.5448	20	2.1598	55.7368
3	synpic42043	11.5566	18	1.5345	55.0100
4	synpic42044	10.7807	21	1.6728	53.2972
5	synpic42057	11.4423	20	1.6004	61.1181
Average			20.2	1.7326	56.3130

Table 4.3 CR, MSE and PSNR

Sr. No	Image(.jpeg)	BER(Bit Error Rate)		Entropy	
		Existing Method	Proposed Method	Existing Method	Proposed Method
1	Synpic48526	1.5000	0.4660	6.9037	6.6968
2	synpic48527	1.5000	0.3875	6.8721	6.5715
3	synpic48528	1.5000	0.4022	7.2541	6.8978
4	synpic48529	1.5000	0.4141	7.1080	6.8642
5	Synpic48530	1.5000	0.4295	6.5841	6.3685
Average			0.41986	6.9444	6.61616

Table 4.4 Comparison of BER and the Entropy with the existing system

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

S. No.	Image (.jpeg) (512x512) Pixels	PSNR of ETC System [1] (Existing method)	PSNR of ECNHWTNS System (Proposed method)
1	Baboon	49.91	51.54
2	Lena	49.89	51.46
3	Boat	49.90	51.53
4	Peppers	49.89	52.34
5	Goldhill	49.89	49.91
Average		49.89	51.35

Table 4.5 Comparison of PSNR with existing technique

Comparison of the Bit Error Rate (BER) values and the Entropy of the previous [1] and the proposed system is shown in the table 4.4 below

Sr. No	Image(.jpeg)	BER(Bit Error Rate)		Entropy	
		Existing Method	Proposed Method	Existing Method	Proposed Method
1	synpic22042	1.5000	0.3131	6.3414	12.6996
2	synpic23691	1.5000	0.3855	6.6679	13.1697
3	synpic29916	1.5000	0.3505	5.4066	10.9849
4	synpic30391	1.5000	0.1238	2.9240	5.3315
5	synpic32212	1.5000	0.3744	5.4837	10.9892
Average			0.30946		10.63498

Table 4.6 Comparison of BER and the Entropy with the existing system

4.2 Graphs

4.2.1 Compression Graph of the previous work and the proposed work is as follow:

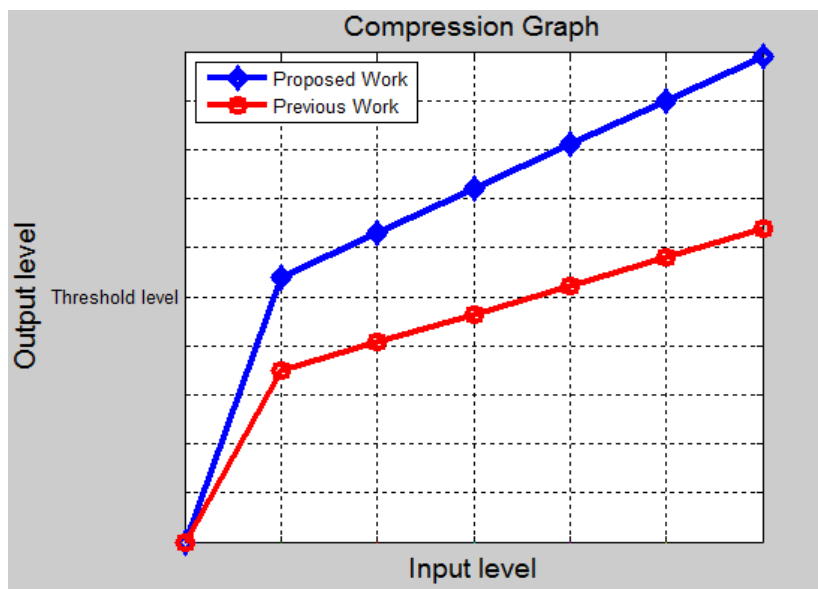


Fig.4.5 Compression graph

4.2.2 Solidity Graph

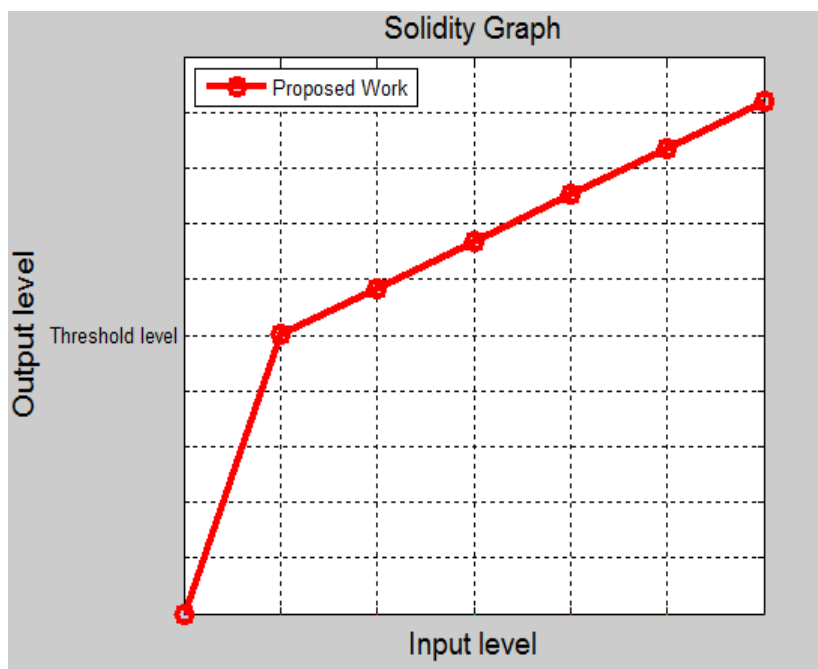


Fig.4.6 Solidity graph

4.2.3 Average PSNR graph of the previous and proposed work

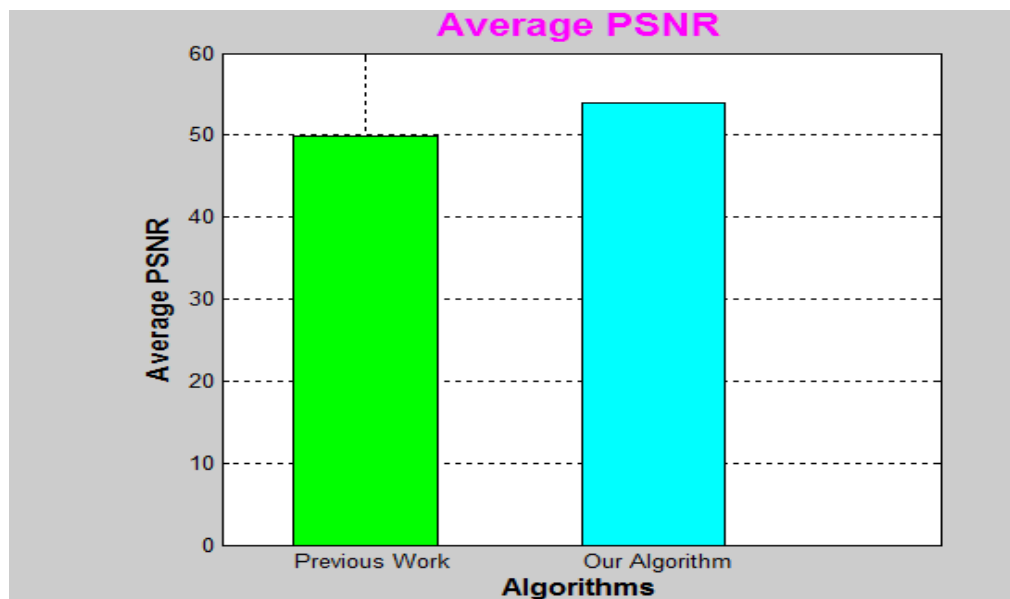


Fig.4.7 PSNR Graph

4.2.4 Average MSE graph of the previous and proposed work

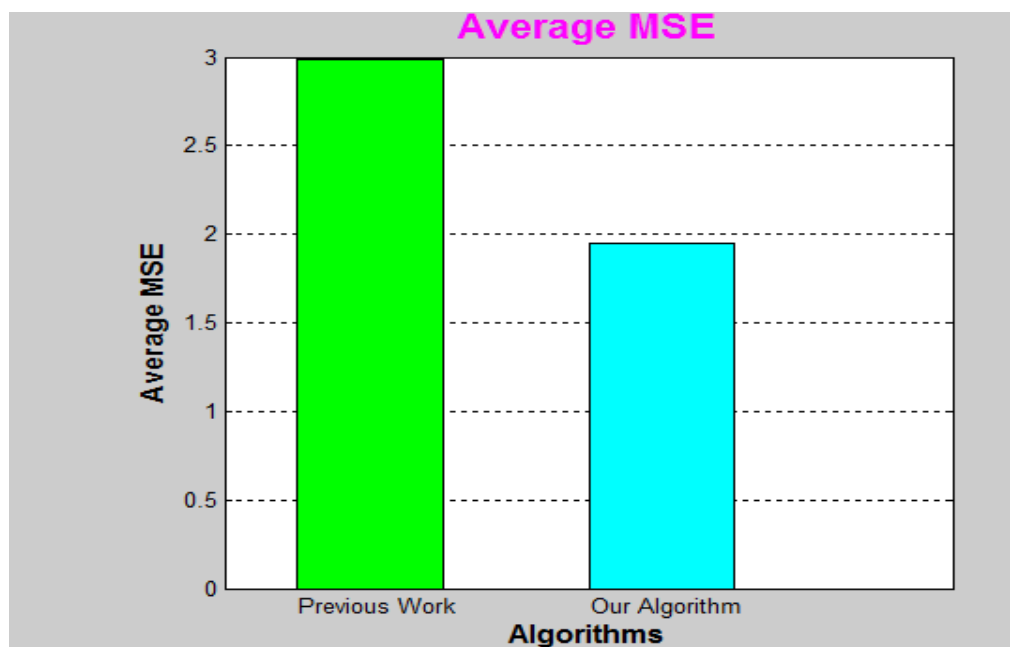


Fig.4.8 MSE Graph

4.2.6 Average Entropy and BER of the previous and the proposed work

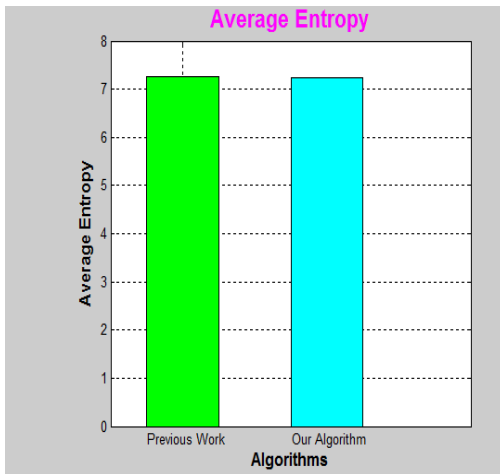


Fig.4.9 Entropy Graph

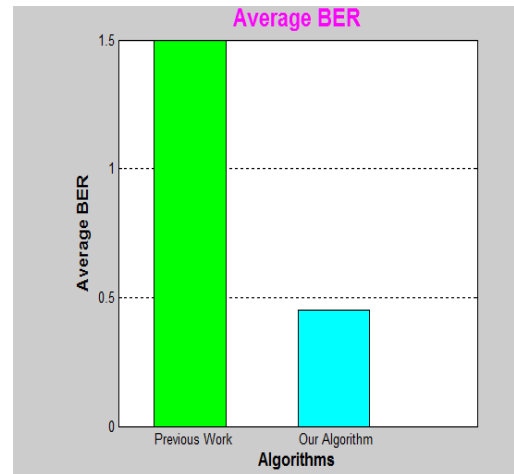


Fig. 4.10 BER GRAPH

4.2.7 Graphs of the various parameters

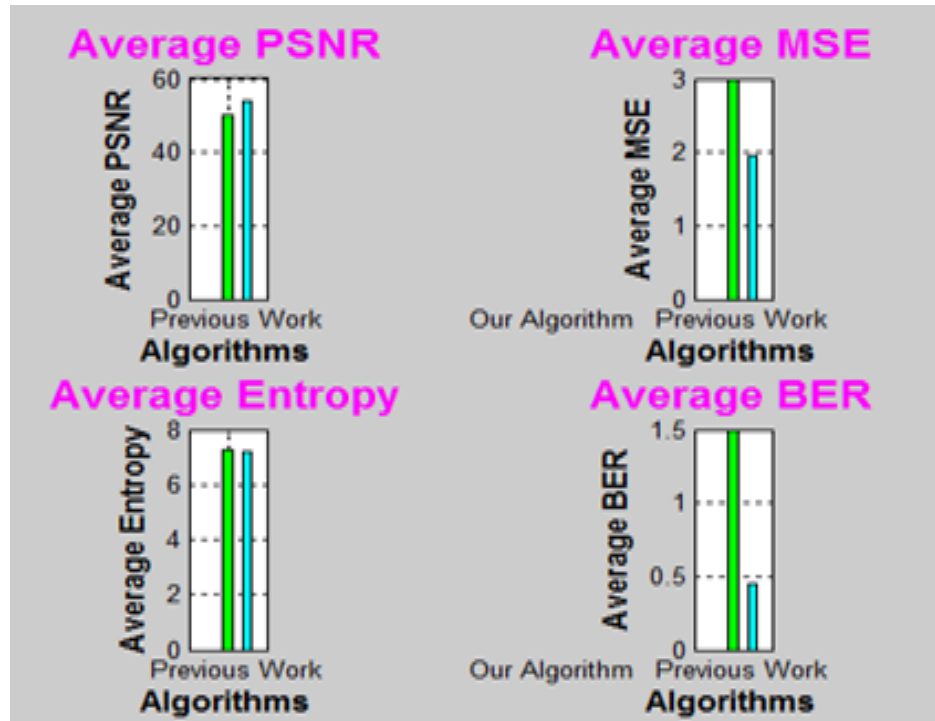


Fig.4.12 Graphs of various parameters

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

This research work designs an efficient image for Encryption and Compression system. Framework of this proposed work, has been achieved the image encryption by random permutation. Therefore, a highly efficient compression of encrypted image realized by a new image compression algorithm of Haar and Symlet wavelet transform. The Experimental result shows the logically high level of security has been retained. The coding efficiency of this proposed compression method on encrypted images is very close to the lossy image codecs which receive original and unencrypted images as input. The images results in terms of PSNR values are better than the previous one. Here, the Better PSNR indicates the reconstruction of image is of higher quality.

5.2 Future Work

For the future, it can be extended with the same technique by applying different transforms to cover image and thus robustness of algorithm can be verified.

- Telemedicine: In medical imaging system, image compression is the important task. All the medical images are of large size and hence the high bandwidth is required for transmission of the medical image. At rural hospitals, there have not that much of required telecommunication infrastructure. Thus the lossless compression can be used at such situations as it has advantage less bandwidth saving required. However, to improve the compression ratio, many studies have been proposed that compression of image can take place in such a way that there will be no any effect on the visual characteristics of the image and it will be easy to transmit with lesser bandwidth.
- In wavelet compression, every of probable combinations of coefficients of the pixel are also considered for reducing the bits.
- Neural Network models may be considered to improve the compression rate.

CHAPTER 6

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 Transactions on Information Forensics and Security, Vol. 9, no. 1, January 2014.
- [2] S.Dharanidharan, S.B.manoojkumaar, D.Senthikumar, “Modified International Data Encryption Algorithm using in Image Compression Techniques”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume2, Issue2, March 2013.
- [3] R.Loganathanand, Dr.Y.S. Kumaraswamy11, “Active Contour Based Medical Image Segmentation and Compression Using Biorthogonal Wavelet and Embedded Zerotree,” Indian Journal of Science and Technology.
- [4] D.Maheswari, Dr. V. Radha, “Improved Block Based Segmentation and Compression Techniques for Compound Images”, International Journal of Computer Science & Engineering Technology (IJCSET).
- [5] Janaki. R, Dr.Tamilarasi.A,“Enhanced Lossy Techniques for Compressing Background Region of Medical Images Using ROI-Based Encoding,” IJCSET |December 2011 | Vol 1, Issue 11, 690-695.
- [6] Ch. Samson, V. U. K. Sastry,V, “ An RGB Image Encryption Supported by Wavelet-based Lossless Compression” , (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.3, No. 9, 2012.
- [7] M. Firoozbakht, J. Dehmeshki, M. Martini, Y. Ebrahimdoost, H. Amin, M. Dehkordi, A. Youannic, SD. Qanadli, “Compression of digital medical images based on multiple regions of interest”.
- [8] Janaki. R, Dr. Tamilarasi. A,” Enhanced ROI (Region of Interest Algorithms) for Medical Image Compression,” International Journal of Computer Applications (0975 – 8887) Volume 38– No.2, January 2012.
- [9] Guiliang Zhu, Zhengzhou, Weiping Wang, Xiaoqiang Zhang, Mengmeng Wang. “Digital image encryption algorithm based on pixels, “Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on (Volume 1).

Encryption-then-Compression System using Haar and Symlet Wavelet Transform

- [10] Ma, K. , Hefei, Weiming Zhang ; Xianfeng Zhao ; Nenghai Yu, “Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption”, Information Forensics and Security, IEEE Transactions on (Volume:8 , Issue: 3)
- [11] RaviShankar, K.C, Venkateshmurthy M,G , “Region based selective image encryption” , IEEE Computing & Informatics, 2006, ICOCI.
- [12] 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 Transactions on Information Forensics and Security, Vol. 9, no. 1, January 2014.
- [13] Bianchi, T., Piva A, Barni A, “On the Implementation of the Discrete Fourier Transform in the Encrypted Domain,” Information Forensics and Security, IEEE transactions on Volume 4, Issue 1.
- [14] Ranu Gupta, “A new image compression algorithm using Haar Wavelet Transformation”, JCSI International Journal of Computer Science Issues, Vol. 11, Issue 2, No. 1, March 2014.
- [15] Xinpeng Zhang, Guangling Sun, Liquan Shen, Chuan Quin, “Compression of encrypted images with multilayer decomposition”, Multimedia Tools and Applications, September 2014, Volume 72, Issue 1, pp 489-502.
- [16] J. Zhou et al., “12 reclamation of l_∞ -decoded images by means of delicate choice estimation.”
- [17] Demijan Klinc, Carmit Hazay, Ashish Jagmohan, Hugo Krawczyk and Tal Rabin, “Compression of data encrypted with block ciphers, such as the Advanced Encryption Standard”
- [18] Erkin, Z, Veugen, T. , Toft T., Lagendijk, R.L. “ Generating Private Recommendations Efficiently using Homomorphic Encryption and Data Packing”, Information Forensics and Security, IEEE Transactions on Volume 7, Issue: 3.
- [19]A. Kumar, Makur, A, “Lossy compression of encrypted image by compressing sensing technique.” TENCON 2009-2009 IEEE Region 10 Conference on Jan. 2009.[20] Miss S.S. Tamboli, Dr. V.R. Udipi “Image Compression using Haar Wavelet Transform. In that paper, Haar Wavelet Transform”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8, August 2012.

- [21] Xinpeng Zhang, Yanli Ren, Guorui Feng, Zhenxing Qian, "Compressing encrypted image using compressive sensing", Intelligent Information Hiding and Multimedia Processing (IIH-MSP), 2011 Seventh International Conference on Oct. 2011.
- [22] Barni. M ,Failla P. , Laxxereti, R. , Sadeghi, A. "Privacy-preserving ECG classification with branching programs and neural networks", Information Forensics and Security, IEEE Transactions on Volume 6, Issue:2.
- [23] Asha P. Ghodake, Sujata Mendgudle, "Modified scheme for Lossy compression and iterative reconstruction for encrypted image." International Journal of Electronics and Computer Technology (IJECT) Vol. 3, Issue 4, Oct- Dec 2012.
- [24] Wei Liu, Zeng, Wenjun, Lina Dong, Qiuming Yao "Efficient compression of encrypted grayscale images", Image Processing, IEEE Transactions on Volume 19, Issue: 4.
- [25] Bianchi. T,Piva .A, Barni.M, "Composite signal representation for fast and storage-efficient processing of encrypted signals." Information Forensics Security, IEEE Transactions on Volume 5, Issue 1.
- [26] V. Ashoka, T. Balakumaran, C. Gowrishankar, I.L.A. Vennila, A. Nirmal Kumar , "The Fast Haar Wavelet Transform for Signal & Image Processing", International Journal of Computer Science and Information Security , IJCSIS January 2010.
- [27] Q.M.Yao, Wenjun Zeng, Wei Liu, "Multi-resolution based hybrid spatiotemporal compression of encrypted videos," Acoustics Speech and Signal Processing 2009. ICASSP 2009, IEEE Conference on April 2009.
- [28]T. Bianchi, Piva, A., Barni, M. "On the implementation of the discrete Fourier transform in the encrypted domain," Information Forensics and Security, IEEE Transactions on Volume 4, Issue 1.
- [29]A. Kumar, Makur, A. "Lossy compression of encrypted image by compressing sensing technique," TENCON 2009-2009 IEEE Region 10 Conference on Jan. 2009.
- [30] T. Bianchi, Piva, A, Barni "Encrypted domain DCT based on homo-morphic cryptosystems," IEEE Transactions on Information Forensics and Security, Volume 4, Issue 1, 2009, pp 86-97.
- [31] D. Schonberg, Draper, S.C., Chuohao Yeo, Ramchandran, K. "Toward compression of encrypted images and video sequences," Information Forensics and Security, IEEE Transactions on Volume 3, Issue 4.

- [32] R. Lazzeretti, Mauro Barni, “Lossless compression of encrypted grey-level and color images,” 16th European Signal Processing Conference (EUSIPCO 2008).
- [33] A. Kumar, Makur, A. “Distributed source coding based encryption and lossless compression of gray scale and color images,” Multimedia Signal Processing, 2008 IEEE 10th workshop on Oct. 2008.
- [34] D. Schonberg, Draper, S.C, Chuohao Yeo, Ramchandran, K. “On compression of encrypted images,” Information Forensics and Security, IEEE Transactions on 2006, Volume 3, Issue 4.
- [35] D. Schonberg, S.C. Draper, K. RamChandran, “On blind compression of encrypted correlated data approaching the source entropy rate.
- [36] K. Wahid, “Error-free computation of 8×8 2D DCT and IDCT using two-dimensional algebraic integer quantization”.
- [37] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, K Ramachandaran, On Compressing Encrypted Data” IEEE Transactions Signal Processing, 2004.
- [38] Piotr Porwik, Lisowsks Agnieszka, “The Haar Wavelet Transform in Digital Image Processing: its status and achievements,” Machine Graphics and Vision, ISSN 1230-0535.
- [39] Bryan Usevitch, “A Tutorial on Modern Lossy Wavelet Image Compression: Foundations of JPEG 2000,” Signal Processing Magazine, IEEE Transactions on Volume 18, Issue 5 in Step 2001.
- [40] Haweel T.I, “a new square wave transform based on the DCT” Signal Processing, Volume 81,Nov. 2011.
- [41] M. J. Weinberger, G. Seroussi, G. Sapiro, “The LOCO-I loss-less image compression algorithm: Principles and standardization into JPEG-LS,” Image Processing ,IEEE Transaction on 2000, Volume 9, No. 8, pp 1309-1324.

CHAPTER 7

APPENDIX

7.1 Abbreviations

CT	Computed Tomography
ETC	Encryption-then-Compression System
GAP	Gradient Adjusted Predictor
MED	Median Edge Detector
CR	Compression Ratio
MSE	Mean squared Error
PSNR	Peak Signal to Noise Ratio
BER	Bit Error Rate
RGB	Red Green Blue
SAHC	Secure Advanced Hill Cipher
DFT	Discrete Fourier Transform
DCT	Discrete Cosine Transform
LDPC	Low Density Parity Check
SQ	Scalar Quantization

CHAPTER 8

PUBLICATIONS

Published Paper:

[1] Navneet Kaur Kang, Sanyam Anand (2015). A comparative study of enhanced ROI techniques, International Journal of Computer Science and Technology, Volume 6, Issue I, Spl-1.

Sent for Review:

[2] Navneet Kaur Kang, Sanyam Anand (2015). Encryption-then-Compression System using Haar and Symlet Wavelet Transform, Indian Journal of Medical Research.