ISSN:2229-6093

K B Shiva Kumar et al, Int. J. Comp. Tech. Appl., Vol 2 (4), 1035-1047

Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques

K B Shiva Kumar [1], K B Raja[2], R K Chhotaray[3], Sabyasachi Pattnaik[4]

[1]Department of TC, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India

[2]Department of ECE, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India

[3]Department of CSE, Seemanta Engineering College, Mayurbhanj, Odisha, India

[4]Department of Computer Science, FM University, Balasore, Odisha, India

kbsssit@gmail.com, raja_kb@yahoo.com,spattnaik40@yahoo.co.in

Abstract

A technique which enables to have a secret communication in modern technology using public channel is known as steganography. In this paper, we propose Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT). The cover image intensity values are manipulated to accommodate payload properly and segmented into blocks of 4*4 each. Discrete Wavelet Transform (DWT) is applied on each block and in the resulting DWT coefficients, blocks of vertical band of 2*2 each are considered and Integer Wavelet Transform (IWT) is applied to get blocks of 1*1 each. The IWT is applied on the DWT vertical band of payload and then embedded into the IWT coefficients of the cover image. The concept of Error Detection and Correction Coding (EDCC) technique is employed to ensure more reliable communication. It is observed that the proposed algorithm has excellent PSNR, provides high level security and more robust compared to individual transform techniques.

***Index Terms*: Steganography, Cover Image, Payload, Stego Image, DWT, IWT and EDCC.**

1. INTRODUCTION

Steganography is a unique technique of hiding data in some medium so that it doesn't arouse suspicion to the hackers. Based on two Greek words, *Steganos* and *graphia*, meaning covered writing, the term steganography has been derived. Another data hiding technique cryptography is a well researched area and has a strong mathematical base in number theory. In cryptography, the secret data is hidden by scrambling it so that it is made unreadable but that might give a clue to the hacker that there is a confidential message. But steganography is concealed writing and it does not draw the attention of an unauthorized person. The brilliance of cryptography did outshine steganography and it was almost neglected by researchers until 1983 when Simmons published a paper in which the principles and benefits of modern digital steganography. Choosing the hiding medium as the criteria, the steganographic techniques are classified as:

(i) *Text-based Steganography* in which the message to be sent is embedded in a text file by formatting it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the embedded content hence the technique is not robust.

(ii)*Audio Steganography* alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding and

(iii) *Image Steganography* hides message in the images. This technique is the most popular because of the fact that almost no perceivable changes occur in images after hiding a large amount of data with wide variety of available images. Depending on the data hidden in the pixels directly or in the coefficients obtained after a suitable transform domain like FFT, DFT or DWT leads to spatial domain steganography and frequency domain steganography. Some of the commonly used methods of embedding payload in cover image are (i) *least Significant Bits (LSB) substitution* in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges. The technique is not robust since alteration of pixel values by channel noise or by hacker corrupts the hidden message. (ii)*Spread Spectrum Steganography* message is spread over wide range of frequencies using pseudo-random noise sequences. (iii) *Color Palette* is generated using color quantization and message is hidden with the help of coding structure. Payload is embedded into the color palette as index of pixel positions around centroids.

(iv) *Transform Domain Steganography* in which the cover image and/or payload are converted into frequency domain and the payload is embedded into the coefficient of cover image to derive stegoimage. Steganography applications are Defense and Intelligence, Law Enforcement and counter-intelligence agencies, copyright protection, Bank Transactions, Medical Field to hide information of a patient.

Contribution: In this paper, PCRSMT is proposed for secret and secure communication. Cover image as well as payloads are applied with DWT and IWT. Most Significant Bits (MSB) of payload IWT coefficients are embedded into Least Significant Bits (LSB) IWT coefficients of cover image. Error Detection and Correction coding technique is also being employed to increase robustness.

Organization: The paper is organized into following sections. Section 2 is an overview of related work. The steganography model is described in section 3. Section 4 discusses the algorithms used for embedding and extracting process. Performance analysis is discussed in section 5 and Conclusion is given in section 6.

2. LITERATURE SURVEY

Bhattacharyya et al.,[1] proposed a specific image based steganography technique for communicating information more securely between two locations by incorporating the idea of secret key for authentication at both ends in order to achieve high level of security. Before the embedding operation the cover image is segmented in different objects through normalized cut. As a further improvement of security level, the information has been permuted, encoded through integer wavelet transformation by lifting scheme and segmented in different parts and then each part has been embedded through modified LSB embedding method on different cuts of the cover image to form different stego objects. Finally stego image is formed by combining different stego objects and transmit to the receiver side. Sarreshtedari and Ghaemmaghami[2] proposed a high capacity method for transform domain image steganography is and algorithm works on the wavelet transform coefficients of the original image to embed the secret data by retaining integrity of the wavelet coefficients at high capacity embedding.

Djebbar et al.,[3] presented a technique that limits the impact of high data capacity embedding on the quality of stego wideband speech. by using the energy of each frequency bin component to determine the maximum number of bits that can be confined without inducing any noticeable distortion on the cover speech. The embedding in the selected frequency components occurs below a well defined distortion level to limit the impact of the hiding on the stego-speech to ensure its good quality. Elham Ghasemi et al., [4] presented the application of Wavelet Transform and Genetic Algorithm in a steganography scheme by employing a genetic algorithm based mapping function to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message and the frequency domain is utilized to improve the robustness of steganography**.** Safy et al., [5] proposed an adaptive steganographic technique in which the bits of the payload are hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm.

Raja et al., [6] proposed a Genetic Algorithm based Steganography using Discrete Cosine Transforms (GASDCT) and Genetic Algorithm based Steganography using Discrete Wavelets Transform (GASDWT). The approach uses the Discrete Cosine Transform and Discrete Wavelet Transform are applied to the payload. Genetic Algorithm is used to generate many stego-images based on Fitness functions; one of these which give least statistical evidence of payload is selected as the best stego image to be communicated to the destination.

Po-Yueh Chen and Hung-Ju Lin [7] proposed a steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and five cases. Unlike the space domain approaches, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Coefficients in the low frequency sub-band are preserved unaltered to improve the image quality. Some basic mathematical operations are performed on the secret messages before embedding. These operations and a well-designed mapping Table keep the messages away from stealing, destroying from unintended users on the internet and hence provide satisfactory security. Hongmei Tang et al., [8] suggested a scheme for image encryption and steganography by encrypting the message with a combination of new gray value substitution operation and position permutation and then it is hidden in the cover image. Gallegos-Funes et al., [9] presented a robust steganographic method for hidden information in the wavelet domain by using the Iterative Center Weighted Median (ICWM) algorithm to estimate the noisy areas of an RGB image. Ghasemi et al.,[10] proposed a novel steganography scheme based on Integer Wavelet Transform and Genetic Algorithm where the scheme embeds data in integer wavelet transform coefficients by using a mapping function based on Genetic Algorithm in an 8×8 block on the cover image. The optimal pixel adjustment process is applied after embedding the message.

Zhang Jiajia et al.,[11] described a steganographic method based on SOM and wavelet contrast to provide large capacity of the hidden secret data and to maintain a good visual quality of stego-image. Firstly, an image was divided into blocks, and every block was decomposed into one-level wavelet to obtain the wavelet contrast. Then, blocks were classified by the Self-organizing Map (SOM) Neural Networks. Finally, the secret information was embedded with steganography based on modulus. Kumar and Muttoo [12] presented a distortionless data hiding technique based on wavelet-like transform, known as Slantlet Transform (SLT). The proposed algorithm first encodes the original message using the encoder, T-codes. T-codes have shown to be more robust than the best known variable-length codes, Huffman codes. T-codes have a well-explained resyhchronization mechanism which leads to fast and reliable resynchronization. The secret data is then embedded in the high frequency sub-bands, viz., HH, HL and LH which are obtained by applying Slantlet transform to the cover-image. Abdelwahab and Hassaan[13] proposed an image data hiding technique based on Discrete Wavelet Transform (DWT) for hiding a secret image S inside a

cover image C using two secret keys to obtain a stego-image G.

Mandal and Sengupta[14] proposed a DWT based frequency domain steganographic technique, termed as WTSIC where the cover PPM image transform into the time domain through DWT, resulting four sub-image components as `Low resolution', `Horizontal orientation', `Vertical orientation' and `Diagonal orientation'. Secret message/image bits stream in varying positions are embedded in all three components. Data Hiding Techniques Based on Wavelet-like Transform and Complex Wavelet Transforms. Kumar and Muttoo[15] compared data hiding techniques based on wavelet-like transform, viz., Slantlet transform, DD DT DWT and Complex Wavelet transforms, viz., DT CWT using wavelet based fusion method and thresholding method. Performance evaluation of DWT based image steganography. Kumar and Kumar [16] observed the effect of embedding the secret message in different bands such as CH, CV and CD on the performance of stegano image in terms of Peak Signal to Noise Ratio (PSNR). Experimentation has been done using six different attacks.

Souvik Bhattacharyya et al., [17] proposed a specific image based steganography technique for communicating information more securely between two locations. The author incorporated the idea of secret key for authentication at both ends in order to achieve high level of security. Before the embedding operation the cover image is segmented in different objects through normalized cut. As a further improvement of security level, the information has been permuted, encoded through integer wavelet transformation by lifting scheme and segmented in different parts and then finally each part has been embedded through modified lsb embedding method on different cuts of the cover image to form different stego objects. Finally stego image is formed by combining different stego objects and transmit to the receiver side. Anjali and Kulkarni[18] presented steganography method based on biometrics and the biometric feature used to implement steganography is skin tone region of images. The secret data is embedded within skin region of image that will provide an excellent secure location for data hiding. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed using frequency domain approach - DWT (Discrete Wavelet Transform), DWT outperforms than DCT (Discrete Cosine Transform). Secret data is hidden in one of the high frequency sub-band of DWT by tracing skin pixels in that sub-band. Hu-Yu Huang and Shih-Hsu Chang[19] proposed a lossless data-hiding scheme based on quantized coefficients of discrete wavelet transform (DWT) in the frequency domain to embed secret message. Using the quantized DWT-based method, secret data is embedded into the successive zero coefficients of the medium-high frequency components in each reconstructed block for 3-level 2-D DWT of a cover-image.

3. MODEL

In this section evaluation parameters, proposed PCRSMT embedding and retrieval techniques are discussed.

3.1 Evaluation Parameters

3.1.1 Mean Square Error (MSE): It is defined as the square of error between cover image and stegoimage. The distortion in the image can be measured using MSE and is calculated using Equation 1.

$$MSE = \left[\frac{1}{N * N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}(X_{ij} - \bar{X}_{ij})^2 \qquad (1)$$

Where:

X_{ij} : The intensity value of the pixel in the cover image.

$\bar{X}_{ij}$: The intensity value of the pixel in the stego image.

N: Size of an Image.

3.1.2 Peak Signal to Noise Ratio (PSNR): It is the measure of quality of the image by comparing the cover image with the stegoimage, i.e., it measures the statistical difference between the cover and stegoimage is calculated using Equation 2.

$$PSNR = 10log_{10}\, 255^2/MSE\ db \qquad (2)$$

3.1.3. Capacity: It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Hiding Capacity (HC) in terms of percentage.

3.2 Proposed PCRSMT Embedding Model:

The proposed embedding model PCRSMT is as shown in figure 1.

3.2.1 Cover-Image (CI):

The cover image is color or gray scale of any size and format. If the cover image is color then convert into gray scale image and corresponding pixel intensity values.

3.2.2 Payload (PL):

The color image of suitable size and different format which is to be transmitted in covert way is considered as a payload.

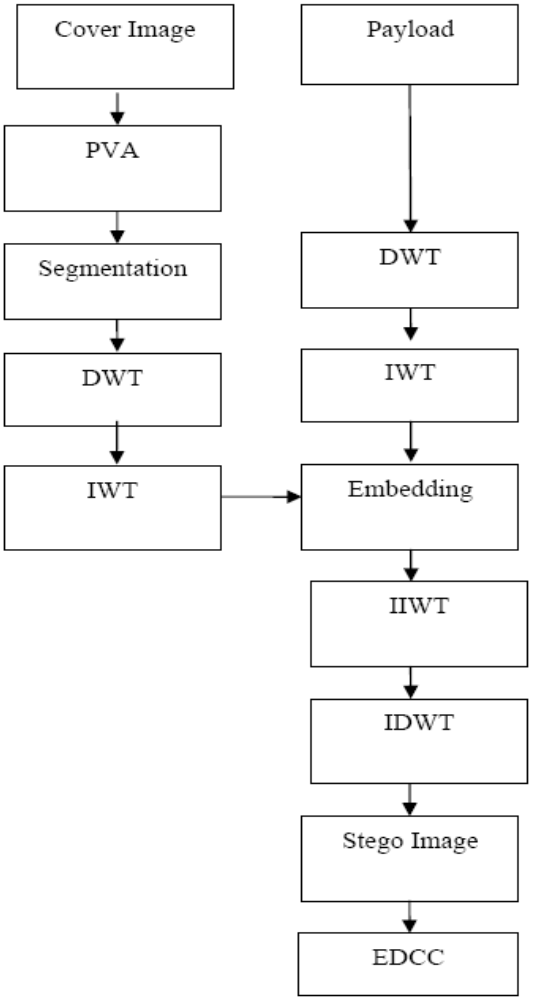

Fig 1: PCRSMT Embedding Model

3.2.3 Pixel Value Adjustment (PVA): The gray scale cover image and payload pixel intensity values vary from *zero* to *255*. During the payload embedding process the intensity values of cover image may exceed lower and higher levels which results in difficulty to retrieve the payload at the destination. Hence the cover image pixel intensity values are limited to lower 15 and upper *240* instead of *zero* and *255*.

3.2.4 Segmentation: The Cover image is divided into blocks each of 4*4 matrix.

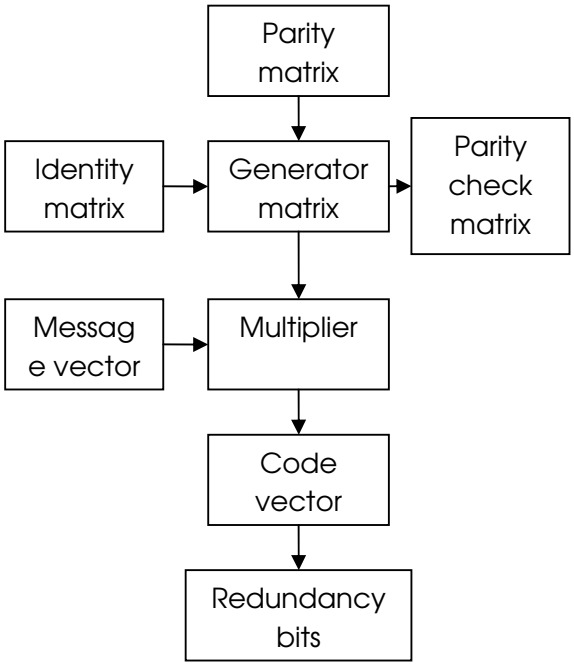

Fig 2: Block diagram for EDCC Encoder.

3.2.5 DWT: In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled with a key advantage over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time). The Haar DWT illustrates the desirable properties of wavelets in general. First, it can be performed in $O(n)$ operations; second, it captures not only a notion of the frequency content of the input, by examining it at different scales, but also temporal content, i.e. the times at which these frequencies occur. The discrete wavelet transform finds applications in science, engineering, mathematics and computer science. Most significantly, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a preconditioning for data compression. It is computationally impossible to analyze a signal using all wavelet coefficients and it is sufficient to pick a discrete subset of the upper half plane to reconstruct a signal from the corresponding wavelet coefficients. The corresponding discrete subset of the half plane consists of all the points with integers m,n € Z . The corresponding *baby wavelets* are now given as

$$\psi_{m,n}(t) = a^{-m/2}\psi(a^{-m}t - nb). \qquad (3)$$

A sufficient condition for the reconstruction of any signal x of finite energy is given by the formula

$$x(t) = \sum_{m \in Z} \sum_{n \in Z} (x, \psi_{m,n}) \psi_{m,n}(t) \qquad (4)$$

In this paper DWT is applied on each 4*4 block to obtain four bands C_a, C_v, C_h and C_d (i.e., approximate, vertical, horizontal and diagonal bands of cover image respectively) of 2*2 each of size 64*64. DWT is applied to payload of size 80*80 to obtain four bands P_a, P_v, P_h and P_d (i.e., approximate, vertical, horizontal and diagonal bands of payload respectively).

3.2.6 IWT: IWT is a non linear transform having a structure of lifting scheme and as its rate distortion performance is similar to DWT, it ensures perfect reconstruction. The floating points of C_v and P_v bands are rounded off to the nearest integer values and then IWT is applied to the vertical band of both cover and payload images to obtain four bands of 1*1 cells each of size 64*64.

3.2.7 Embedding Process: The IWT coefficients of payload are embedded into the IWT coefficients of the cover image.

3.3.8 IIWT & IDWT: After embedding apply inverse IWT and inverse DWT to derive stegoimage.

3.2.9 Error correction and detection coding: Error detection and correction coding structure [20] is employed to provide authenticity and error free secure communication. The block diagram of the EDCC encoder is as shown in figure 2.

ENCODER:

Parity matrix [P]: The parity matrix is an arbitrary matrix of order (k) X (n-k)

Where k is the length of the message vector

n is the length of the code vector

There are certain rules that are to be considered while assuming the parity matrix. They are:

1. No two rows of [P] must be same, i.e., all rows of [P] must be distinct.

2. [P] Should not contain a row of zeros as it represents the syndrome of no error.

3. [P] Should not contain the elements of identity matrix.

It is suitably selected to correct one bit error in any of the four LSB's. In this paper the order of the parity matrix is 4 X 3. There are totally $2^{(n-k)}$ combinations namely 000, 001, 010, 011,100, 101, 110, 111. Out of these eight combinations 000, 001, 010 and 100 cannot be used as it does not satisfy the above conditions. We select only four combinations 011, 101, 110 and 111 as the four rows of [P]. Thus we have 4!=24 ways of representing these combinations as rows of [P]. Any one of the 24 combinations is selected.

Generator matrix [G]: Generator matrix of the order kXn is created by concatenating identity matrix [I] of order k X k and parity matrix.

$$[G] = [P \mid I]$$

$$(G) = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Parity check matrix [H]: It is obtained by concatenating the transpose of parity matrix with identity matrix of order (n-k) X n. This matrix is used for error correction.

$$(H)^T = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Message vector: In each plane of the stego image, the pixels are converted into binary form having 8 bits. The last four bits are extracted from each pixel which forms the message vector.

Code vector: The message vectors are multiplied with the generator matrix [G] to obtain code vector. Here we get three redundancy bits for each pixel which is sent to the receiver.

For example: if the message vector is [1 0 1 0]. When multiplied with the generator matrix we get

[1 0 1 0 1 0 1] as the code vector.

Hence we get the code vector for all the pixels of the stego image in each plane.

At the receiver, the modified stego image might be obtained due to error in the transmission channel. The

sender provides the necessary parity check matrix and the redundancy bits to the receiver in order to correct and detect the error in the modified stego image.

The modified stego image pixels are converted to binary form and only the four LSBs are extracted. These four LSBs are concatenated with the redundancy bits to get code vector. Thus obtained code vector is multiplied with transpose of the parity check matrix to get syndrome vector.

In the example given below assume the received vector to be [R]=[1 1 1 1 0 0 1]. When this is multiplied with the transpose of parity check matrix $[H^T]$ we obtain syndrome vector as [1 1 0] which is present in the third row of $[H^T]$. Hence the error present in the a third bit of the received vector and can be represented as
[E]= [0 0 1 0 0 0 0]. This is the error vector.

$$[S] = [R][H]^T$$

$$(S) = \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$$

The corrected code vector is obtained by XORing received code vector with the error vector. Thus we obtain the corrected code vector. By doing this we have rectified the one bit error in any of the four LSBs of the stego image.

$$(R) = (1\,1\,1\,1\,0\,0\,1) \oplus (0\,0\,1\,0\,0\,0\,0)$$

$$= (1\,1\,0\,1\,0\,0\,1)$$

The four LSBs of the stego image are replaced with four MSBs of received code vector .This is done for all the pixels of the modified stego image in order to get the original stego image.

3.3 Proposed PCRSMT Extraction Model:

The extraction of payload from stegoimage is a step by step process and is as shown in figure 3.

3.3.1. Stego Image: The payload is embedded into the cover image using PCRSMT technique with DWT and IWT to obtain stego image.

3.3.2. EDCC: The modified stego image pixels are converted to binary form and only the four LSBs are extracted. These four LSBs are concatenated with the redundancy bits to get code vector. Thus obtained code vector is multiplied with transpose of the parity check matrix to get syndrome vector.

3.3.3. Extraction of payload bits: The corrected code vector is obtained by XORing received code vector with the error vector.

3.3.4 Extracted Payload (EPL): The extracted payload coefficients in transform domain are converted into spatial domain bits by applying IIWT and IDWT.

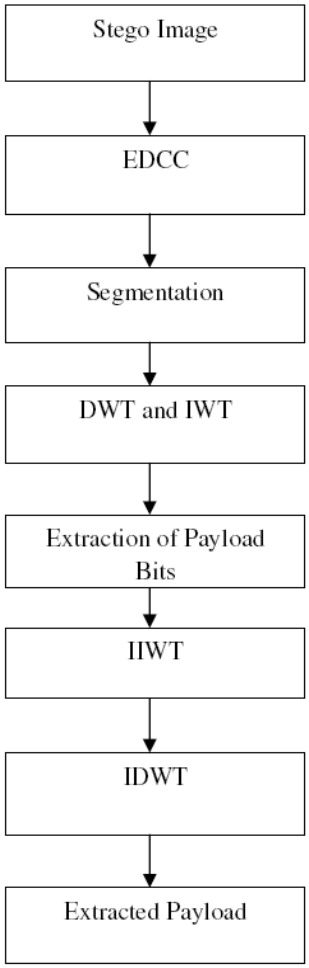

Fig 3: PCRSMT Extraction Model

4. Algorithm:

The embedding and retrieval of payload using PCRSMT algorithm is discussed in this section.

Problem definition: Given cover image and the payload, the objectives are:

1. To embed the payload into the cover image to derive stego image for covert communication.
2. High robustness with reasonable PSNR.

4.1 Embedding Algorithm: The payload is embedded in the cover image using LSB technique. The cover image matrix is divided into blocks of 4*4 each. DWT and IWT are applied and the payload is embedded into IWT coefficients of cover image. The algorithm is given in Table 1.

4.2 Extraction Algorithm: The payload is extracted from the PCRSMT embedded stego image through the retrieval process by performing exactly the inverse process of the embedding technique and the algorithm is given in Table 2.

Table 1: Embedding Algorithm

- Input: Cover image , Payload
- Output: Stego image

(i) Read the cover image and payload images
(ii) Divide the cover image into blocks of 4*4 each.
(iii) Apply DWT to each block to obtain four bands of DWT coefficients of 2*2 cells each, ie., approximate (Ca), vertical (Cv), horizontal (Ch) and diagonal (Cd) bands.
(iv) On applying DWT to payload, four bands, Pa, P_v, P_h and P_d are obtained. The floating point values of C_v and P_v are rounded off to the nearest integer values.
(v) The blocks of vertical band of 2*2 each are isolated both in cover image and payload and IWT is applied to get blocks of 1*1 each.
(vi) The IWT coefficients of payload are embedded into IWT coefficients of cover image.
(vii) After embedding apply inverse IWT and inverse DWT to derive stegoimage.
(viii) Error detecting and correcting coding structure is employed to provide authenticated and error free secure communication.

5. Performance Analysis

The evaluation parameter PSNR and capacity are used as performance analysis factors to verify the image quality between cover image and stego image as well as between payload and extracted payload. The PCRSMT algorithm is tested for different kinds of cover images and payloads with different sizes and formats.

Few cover images and payloads are shown in Figure 5 for the demonstration purpose. PSNR and capacity values between cover image and stegoimage with different sizes and formats by applying different transform domain techniques such as DWT, IWT and PCRSMT are compared in Tables 3, 4 and 5.

The PSNR values between payload and extracted payload with error, without error and with error detection and correction for various combinations of payload and cover image formats by applying IWT and PCRSMT are compared in the Tables 6, 7 and 8.

It is observed that the value of PSNR is better in the case of PCRSMT among pure transform domains DWT and IWT. The proposed technique uses a combination of both DWT and IWT domains by applying DWT and IWT to cover image and payload. By applying IIWT and IDWT, stegoimage is derived.

Concept of error detection and correction coding techniques is also being employed to ensure more reliable communication.

The proposed steganography algorithm is robust as error detection and correction coding technique is being employed.

Table 2: Extraction Algorithm

- Input: Stego Image
- Output :Payload

(i) The decoding technique with EDCC structure is employed to ensure the received bits are error free in the stego image.
(ii) Divide the Stego image matrix into blocks of 4*4 each.
(iii) Apply DWT to each block to obtain DWT coefficients.
(iv) The blocks of vertical band of 2*2 each are separated and IWT is applied to get blocks of 1*1 each.
(v) The bits are taken out from vertical band and placed in diagonal band.
(vi) Apply inverse IWT and inverse DWT to obtain retrieved payload.

Table3: PSNR Comparison of CI and SI of DWT, IWT and PCRSMT with JPEG Images

Cover Image(CI) 256*256 Payload(PL)	DWT		IWT		PROPOSED PCRSMT	
	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI
CI: Lilly PL: Football (80*80)	0.0976	47.6291	0.0976	47.4812	0.0976	47.7162
CI: arraras PL: mandril (90*90)	0.1235	43.2476	0.1235	43.1733	0.1235	43.2719
CI: peppers PL: lena (100*100)	0.1525	50.1743	0.1525	49.7654	0.1525	50.3020
CI: goldhill PL: f14 (110*110)	0.1846	29.5627	0.1846	29.5546	0.1846	29.5638
CI: arctic PL: Audrey (128*128)	0.25	24.5754	0.25	24.5609	0.25	24.5766

Table4: PSNR Comparison of CI and SI of DWT, IWT and Dual Transform with PNG Images

Cover Image(CI) 256*256 Payload(PL)	DWT		IWT		PROPOSED PCRSMT	
	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI
CI: Greatwall PL: James (80*80)	0.0976	55.3598	0.0976	54.6047	0.0976	55.9255
CI: Boatman PL: pout (90*90)	0.1235	32.1717	0.1235	32.1597	0.1235	32.1787
CI:cameraman PL: rice (100*100)	0.1525	43.6678	0.1525	43.5921	0.1525	43.6999
CI: Barbara PL: Rainbow (110*110)	0.1846	58.1481	0.1846	55.5321	0.1846	59.3351
CI: Box PL: tire (128*128)	0.25	42.2482	0.25	42.1050	0.25	42.3012

Table5: PSNR Comparison of CI and SI of DWT, IWT and Dual Transform with TIFF Images

Cover Image(CI) 256*256 Payload(PL)	DWT		IWT		PROPOSED PCRSMT	
	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI	Capacity	PSNR CI&SI
CI: peppers PL: lena (80*80)	0.0976	50.3516	0.0976	50.1119	0.0976	50.4322
CI: Goldhill PL: boat (90*90)	0.1235	55.4491	0.1235	54.4269	0.1235	55.8643
CI: newsecret PL:Barbara (100*100)	0.1525	37.0782	0.1525	37.0582	0.1525	37.0895
CI: flinstones PL: picture1 (110*110)	0.1846	31.4620	0.1846	31.4452	0.1846	31.4714
CI: concord PL: flinstones (128*128)	0.25	51.1029	0.25	50.1659	0.25	51.4788

Table6: PSNR Comparison of PL and EPL after introducing error with JPEG Images

Cover Image(CI) 256*256 Payload(PL)	DWT			IWT			PROPOSED PCRSMT		
	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC
CI: peppers PL: lena (80*80)	0.0976	34.1102	12.8537	0.0976	33.6315	19.0938	0.0976	33.7971	23.1890
CI: Goldhill PL: boat (90*90)	0.1235	34.9704	15.6155	0.1235	34.3417	17.9380	0.1235	35.0985	23.4276
CI: newsecret PL:Barbara (100*100)	0.1525	35.5429	12.5623	0.1525	34.7759	18.7553	0.1525	34.1535	23.4833
CI: flinstones PL: picture1 (110*110)	0.1846	34.7362	11.8455	0.1846	33.9561	17.8212	0.1846	36.2403	23.1042
CI: concord PL: flinstones (128*128)	0.25	20.8856	12.0382	0.25	20.9804	16.7326	0.25	25.7724	22.4101

Table7: PSNR Comparison of PL and EPL after introducing error with PNG Images

Cover Image(CI) 256*256 Payload(PL)	DWT			IWT			PROPOSED PCRSMT		
	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC
CI: Lilly PL: Football (80*80)	0.0976	39.1317	12.5600	0.0976	38.3335	17.9643	0.0976	39.8441	23.0341
CI: arraras PL: mandril (90*90)	0.1235	36.0360	12.1228	0.1235	35.0519	18.8022	0.1235	36.3311	23.6157
CI: peppers PL: lena (100*100)	0.1525	36.6658	12.8046	0.1525	36.0134	19.2123	0.1525	36.3373	23.5238
CI: goldhill PL: f14 (110*110)	0.1846	42.2761	12.3888	0.1846	41.6176	18.5560	0.1846	39.2886	24.4065
CI: arctic PL: Audrey (128*128)	0.25	33.6105	17.1572	0.25	33.0659	22.7441	0.25	34.5003	26.4555

Table8: PSNR Comparison of PL and EPL after introducing error with TIFF Image

Cover Image(CI) 256*256 Payload(PL)	DWT			IWT			PROPOSED PCRSMT		
	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC	Capacity	PSNR with EDCC	PSNR without EDCC
CI: Greatwall PL: James (80*80)	0.0976	37.2284	12.1770	0.0976	36.5801	19.1968	0.0976	37.5714	23.4611
CI: Boatman PL: pout (90*90)	0.1235	42.0811	11.7942	0.1235	41.5643	17.7976	0.1235	40.5877	23.8105
CI:cameraman PL: rice (100*100)	0.1525	35.4643	12.2706	0.1525	35.4101	18.2784	0.1525	34.3817	23.7043
CI: Barbara PL: Rainbow (110*110)	0.1846	32.0990	14.0851	0.1846	31.7328	19.4683	0.1846	35.3459	23.8138
CI: Box PL: tire (128*128)	0.25	36.5043	13.6288	0.25	36.1018	19.4906	0.25	36.5647	24.3232

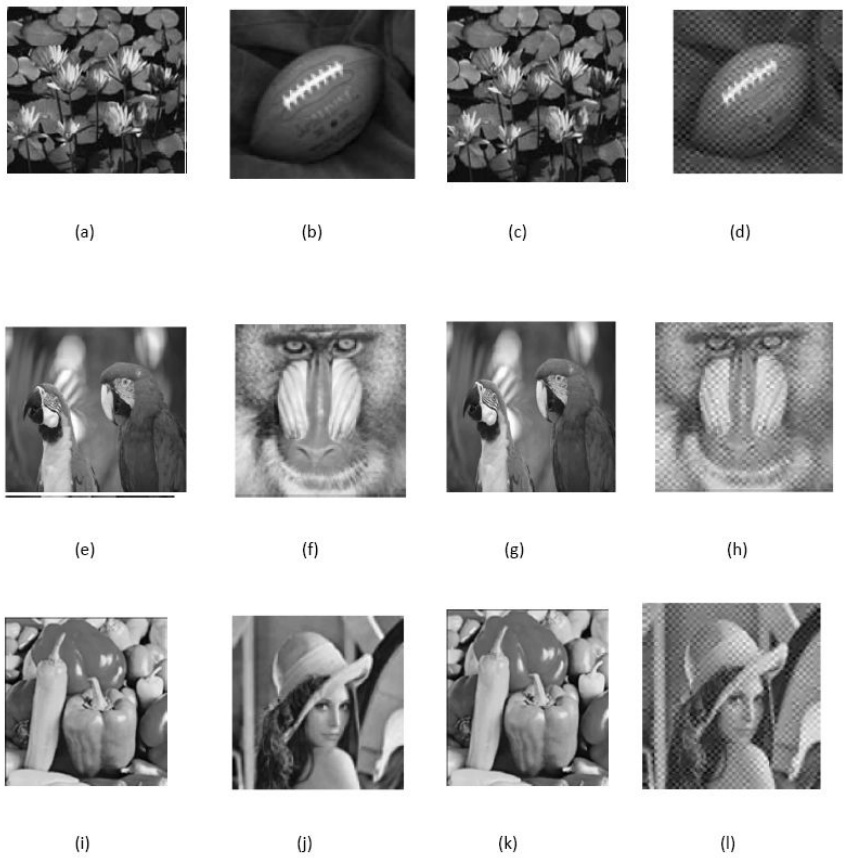

Fig 5: Cover Images :(a), (e),(i), Payloads: (b),(f),(j), Stegoimages: (c),(g),(i), Extracted Images: (d),(h),(k)

6. Conclusions:

Steganography is a technique of hiding messages in some medium so that it doesn't arouse suspicion to the hackers. In this paper, PCRSMT algorithm is proposed. The cover image is divided into 64 blocks of 4*4 each and DWT is applied to each block. The resulting 64 blocks of vertical band of 2*2 each are isolated and IWT is applied to get 1*1 blocks. The DWT and IWT are applied to payload and IWT coefficients of payload are embedded with that of cover image. IDWT and IIWT are applied to derive stego image. In addition error detection and correction technique is also applied to ensure more secured communication. It is observed that the robustness and capacity are improved with very little tradeoffs in PSNR. The proposed technique ensures more security than individual transformation techniques In future; the payload can be embedded in the spatial domain as well as in multiple transformation domains of cover image to increase the security level.

REFERENCES:

[1]Bhattacharyya S Kshitij and A P Sanyal G, "A Novel Approach to Develop a Secure Image Based Steganographic Model using Integer Wavelet Transform," International Conference on recent Trends in Information, Telecommunication and Computing, pp.173-178, 2010.

[2]Sarreshtedari S and Ghaemmaghami S, "High Capacity Image Steganography in Wavelet Domain," International Conference on Consumer Communications and Networking, pp.1-6, 2010

[3]Djebbar F, Hammam H, Abed Meraim K and Guerchi D, "Controlled Distortion for High Capacity Data in Speech Spectrum Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 212-216, 2011.

[4]Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," International MultiConference of Engineers and Computer Scientists, vol. 1, 2011

[5]R O El Safy, H H Zayed and A El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," International Conference on Networking and Media Convergence, pp.111-117, March 2009.

[6]K B Raja et al., "Genetic Algorithm based Steganography using Wavelets," Third International Conference on Information

Systems Security (ICISS2007), LNCS, Springer, pp.51 63, December 2007.

[7]Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography," International Journal of Applied Science and Engineering, pp. 275-290, 2006.

[8]Hongmei Tang, Gaochan Jin, Cuixia Wu and Peijiao Song, "A New Image Encryption and Steganography Scheme," IEEE International Conference on Computer and Communication Security, pp. 60 – 63, 2010.

[9]Gallegos-Funes F J, Carvajal-Gamez B E, Lopez-Bonilla JL, Ponomaryov, "Steganographic Method Based on Wavelets and Center Weighted Median Filter," International Kharkov Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW),pp. 1-3, 2010

[10]Ghasemi E, Shanbehzadeh J and ZahirAzami B, "A steganographic method based on Integer Wavelet Transform and Genetic Algorithm,"International Conference on Communications and Signal Processing (ICCSP), pp. 42-45, 2011

[11]Zhang Jiajia, Liu Jing and Deng Cheng, "A Steganographic Method Based on SOM and Wavelet Contrast," International Conference on Artificial Intelligence and Computational Intelligence, pp 482-484, 2009.

[12]Kumar S and Muttoo, S." Distortionless Data Hiding Based on Slantlet Transform," International Conference on Multimedia Information Networking and Security, pp. 48 - 52, 2009.

[13]Abdelwahab A A and Hassaan L A, "A discrete wavelet transform based technique for image data hiding," National Radio Science Conference, pp. 1-9, 2008.

[14]Mandal J K and Sengupta M, " Authentication/Secret Message Transformation through Wavelet Transform Based Subband Image Coding," International Symposium on Electronic System Design pp. 225 – 229, 2010

[15]Kumar S and Muttoo S K "Data Hiding Techniques Based on Wavelet-like Transform and Complex Wavelet Transforms, International Symposium on Intelligence Information Processing and Trusted Computing , pp. 1 - 4 , 2010.

[16]Kumar V and Kumar, "Performance evaluation of DWT based image steganography," International Advance Computing Conference, pp.223-228, 2010.

[17]Souvik Bhattacharyya, Avinash Prasad Kshitij and GautomSanyal, "A Novel Approach to Develop a Secure Image based Steganographic Model using Integer Wavelet Transform," International Conference on Recent Trends in Information, Telecommunication and Computing , pp.21-25, 2010.

[18]Anjali A. Shejul U.L. Kulkarni, "A DWT Based Approach for Steganography Using Biometrics," International Conference on Data Storage and Data Engineering, pp.10-15, 2010.

[19]Hu-Yu Huang Shih-Hsu Chang, "A Lossless Data Hiding based on Discrete Haar Wavelet Transform," International Conference on Computer and Information Technology, pp.9-14, 2010.

[20]K Giridhar, "Information Theory and Coding," Pooja Publications, 2009-10.

ShivaKumar K B received the BE degree in Electronics & Communication Engineering, ME degree in Electronics, MBA from Bangalore University, Bangalore and MPhil from Dravidian University Kuppam. He is pursuing his Ph.D. in Information and Communication Technology of Fakir Mohan University, Balasore, Odisha under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Dr.Sabyasachi Pattanaik Reader & HOD, Department of Information and Communication Technology F M University, Balasore, Odisha R K Chhotaray, Principal, Seemantha Engineering College, Odisha. He has got 27 years of teaching experience and has over 30 research publications in National and International conferences and journals. Currently he is working as Professor, Dept. of Telecommunication Engineering, Sri Siddhartha Institute of Technology, Tumkur. His research interests include Signal processing, Multi rate systems and filter bags, and Steganography.

Dr. K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He has been awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has got 25 years of teaching experience and he has over 60 research publications in refereed International Journals and Conference Proceedings. Currently he is guiding 10 Ph D scholars in the field of image processing. He has received Best Paper Award for the contributed paper in Fourteenth IEEE-ADCOM 2006. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.

Dr. Sabyasachi Pattnaik has done his B.E in Computer Science, M Tech., from IIT Delhi. He has received his Ph D degree in Computer Science in the year 2003 & now working as Professor in the Department of Information and Communication Technology, in Fakir Mohan University, Vyasavihar, Balasore, Odisha, India. He has got 20 years of teaching and research experience in the field of neural networks, soft computing techniques. He has got 50 publications in National & International journals and conferences. He has published three books in office automation, object oriented programming using C++ and artificial intelligence. At present he is involved in guiding 8 Ph D scholars in the field of neural networks, cluster analysis, bio-informatics, computer vision & stock market applications. He has received the best paper award & gold medal from Odisha Engineering congress in 1992 and institution of Engineers in 2009.

Dr. R K Chhotaray received B.Sc Engineering in Electrical Engineering and M.Sc Engineering in Electrical Engineering with specialization in Control Systems from Banaras Hindu University, and Ph D in Control Systems from Sambalpur University. He was Professor and Head of Department of Computer Science and Engineering, Regional Engineering College, Rourkela, from which he retired in 2003. Currently he is working as Principal of Seemanta Engineering College, Odisha. He has been associated with many Universities of India in the capacity of Chairman and member of various Boards of Studies, syllabus committee, and Regulation committee. He has about hundred publications in International and National journals of repute, and has received Best Technical Paper award in many occasions. His special fields of interest include Control of Infinite dimensional Hereditary Systems, Modeling and Simulation, Theoretical Computer science, signal and Image processing, and optimization.