Wavelet based Non LSB Steganography

H S Manjunatha Reddy
Department of ECE, Global Academy of Technology, Bangalore-98, India
Email: manjunathareddyhs@rediffmail.com
K B Raja
Department of ECE, Bangalore University, Bangalore, India.
Email: raja_kb@yahoo.com

ABSTRACT

Steganography is the methods of communicating secrete information hidden in the cover object. The messages hidden in a host data are digital image, video or audio files, etc, and then transmitted secretly to the destination. In this paper we propose Wavelet based Non LSB Steganography (WNLS). The cover image is segmented into 4*4 cells and DWT/IWT is applied on each cell. The 2*2 cell of HH band of DWT/IWT are considered and manipulated with payload bit pairs using identity matrix to generate stego image. The key is used to extract payload bit pairs at the destination. It is observed that the PSNR values are better in the case of IWT compare to DWT for all image formats. The algorithm can’t be detected by existing steganalysis techniques such as chi-square and pair of values techniques. The PSNR values are high in the case of raw images compared to formatted images.

Keywords - Cover Image, DWT, Multiplier, Payload, Steganography, IWT

Date of Submission: August 17, 2011 Date of Acceptance: September 28, 2011

1. Introduction

Steganography is a branch of art and science of writing secrete messages in such a way that no one except sender and recipient, suspects the existence of the secrete message. The word steganography [1] is origin of Greek word means concealed writing. ie steganos means *covered* or *protected* and graphei means *writing*. The term steganography was originally used as a synonym for data hiding schemes for embedding messages in a cover object. Steganalysis is useful tool for covert transmission over a covert communication channel. It enables the users to transmit message masked inside a file in plain view. The hidden data is difficult to detect by using known steaganalysis algorithms. In general steganography brings both science and technology to the art of hiding messages. Steganography uses an illusion of normality to mask the existence of data. The basic principle of steganography is to ensure that modifications to the data in the cover file must have insignificant bits so that nature of the cover does not differ. The main advantage of steganography over cryptography is that messages do not attract attention to hackers. The cryptography protects only contents of messages where as steganography [2] can protect both messages and its existence in the communication channel.

The steganographic techniques are broadly classified as (i) Spatial domain embedding and (ii) Transform domain embedding. Spatial domain approach embeds messages in the intensity of image pixels directly. Where as in the transform domain the images are transformed into frequency domain and then message are embedded in transformed coefficients. The requirements of steganographic system are Transparency, more capacity and Security and Robustness.

Commonly used methods of embedding payload in cover image are (i) *Least Significant Bits (LSB) substitution*: The LSBs of cover image pixel are replaced without modifying the complete cover object 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 adversary corrupts the hidden message. (ii)*Spread Spectrum Steganography*: The message is spread over wide range of frequencies using pseudo-random noise sequences. (iii) *Colour Palette* is generated using colour quantisation and message is hidden with the help of coding structure. Payload is embedded into the colour palette as index of pixel positions around centroids. (iv) *Transform Domain Steganography:* The cover image and/or payload are converted into frequency domain and the payload is embedded into the coefficient of cover image to derive stego image. The various transform domain techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) and Integer Wavelet Transform (IWT).

Steganography applications are Copyright control of materials, Smart ID cards, medical records, banking and financial Companies data safe circulation, TV broadcasting etc.

Contribution: **I**n this paper cover image is segmented into 4*4 cells. Apply wavelet transform on each cell. The I_M

obtained from identity matrix and payload bit pair, is multiplied by 2*2 valid cover image matrixes to generate stego image.

Organization: **T**he paper is organized into following sections. Section 1 gives Introduction and Section 2 is an overview of the related work. The steganography model is described in section 3.Section 4 discusses the algorithms used for embedding and extracting process and Section 5 discusses the performance analysis and results.

2. Related work

Hongmei Tang et al., [3] proposed a image encryption and Steganography scheme. The combination of a gray value substitution operation and position permutation encrypts the secret message. R O El Safy et al., [4] proposed an adaptive steganographic technique based on integer wavelet transform for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the Optimum pixel adjustment algorithm. To increase the security of hidden data the coefficients used are selected according to a pseudorandom function generator. Nedal Kafri and Hani Suleiman [5] proposed Bit-4 of Frequency Domain-DCT Steganography Technique. This method is based on embedding message bits in the fourth bit of the coefficients of a transform domain, such as DCT and Wavelet of an image. The used technique utilizes the idea of Single Side Band (SSB)-4 technique in modifying the other bits (i.e., 1st, 2nd, 3rd and/or 5th), to obtain the minimum variation between the original and the modified coefficient. Since this approach uses significant bit, the hidden message resides in more robust areas, spread across the entire Stego image, and provides better resistance against Steganalysis processes.

Hang-ling zhang et al., [6] proposed image Steganography using pixel-value differencing to increase the capacity of the hidden secret information and to provide a Stego-image imperceptible for human vision. To estimate how many secret bits will be embedded into the pixel, this approach uses the largest difference value between the other three pixels close to the target pixel. Saeed Sarreshtedari et al., [7] proposed One-third probability embedding that is less detectable LSB Steganography reduces the probability of change per pixel to one-third without sacrificing the embedding capacity. Each bit of the message is carried through a function of three adjacent cover pixels. Ravuru Rakesh et al., [8] Proposed a five different randomization methodologies by adapting an embedding the data in to the bits of Least Significant Nibble (LSN) pertaining to bits in Most Significant Nibble (MSN). The methodologies are (1) Embedding the data in the LSN's according to the ranked order of MSN. (2) uses the reversible property of XOR to implement keyless random approach. Here each 4 bits of data is XORED with MSN and then substituted in LSN. (3) Employing random embedding lengths in each pixel. The number of message bits to be embedded in LSN is varied according to data bits in MSN. (4) The data is embedded in to LSN based on parity of MSN i.e. the number of one's /zeros even or odd. (5) Embedding data in the LSN bits based on the MSN bits are one or zero.

Dipti Kapoor Sarmah et al., [9] have developed a security module by combining both Cryptography and Steganography. In Cryptography uses advanced encryption standard algorithm to encrypt a message and a part of the message is hidden in DCT of an image and remaining part of the message is used to generate a secret keys. Anitha et al., [10] have developed an algorithm by combining the SDES algorithm and Back propagation algorithm of neural network which will effectively detect the stego content in the images. It consists of Image separation from corporate mails using capturing algorithm, Compression, encryption, hiding, decryption, and decompression steps. Manjunath Gadiparthi et al., [11] have proposed a technique which is a combination of PVD modulus and LSB method. The LSB method for smooth areas and Pixel-value differencing method for edge area pixel pairs and they define a threshold to determine whether a pixel pair falls in smooth area or edge area. . Chiew Kang Leng et al., [12] have proposed a technique for hiding information in images through reparation technique in frequency domain. In reparation process, before a particular DCT coefficient is embedded with message bit, the initial value and the altered value of this coefficient is stored and used as the criteria for the reparation. This technique is able to hide message in a JPEG image file and is capable to keep the image frequency differences to a minimum level that can withstand chi-square statistic test. K B Raja et al., [13] have proposed an effective tool called pixel pair analysis using fixed threshold for detecting LSB steganography. The threshold value is evaluated using both the cover image and the stego image and then, based on statistical measures of pixel pairs, the length of the embedded message is computed

3. Model

In this section definitions of evaluation parameters and proposed embedding and retrieval system are described.

3.1. Evaluation Parameters

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

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

Where
X(i,j): Cover image pixel intensity value.
Y(i,j): Stego image pixel intensity value.
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 stego image, i.e., it gives the statistical difference between the cover image and stego image and it is calculated using Equation (2).

$$PSNR = 10\log_{10} \frac{255^2}{MSE}\ dB \qquad (2)$$

3.1.3. Capacity**:** It is the size of the secret message embedded 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 WNLS Embedding Technique

The proposed WNLS embedding algorithm is shown in Figure 1. The cover image is segmented into 4*4 cells and DWT/IWT is applied on each cell to form 2*2 sub band matrices. The embedding process is performed on Horizontal band of DWT/IWT.

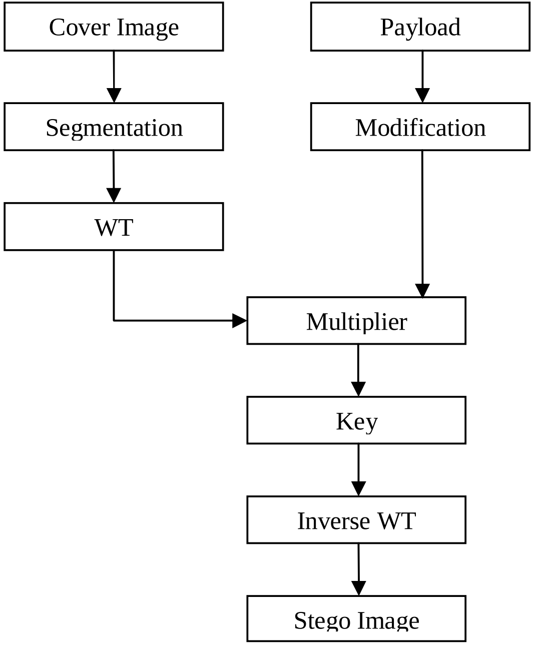


Figure1. WNLS embedding system

3.2.1. Cover Image (CI)**:** It carries original secret information. The different formats like raw images, JPEG, BMP, TIFF and PNG are considered to test the algorithm with different sizes.

3.2.2. Payload (PL)**:** It is the secret information that can be embedded into the cover image to generate stego image.

3.2.3. Segmentation**:** The cover image is decomposed into matrix of size 4*4 to enhance the security to the payload.

3.2.4. Wavelet Transform (WT)**:** The two dimensional DWT/IWT applied on each 4*4 matrix of cover image to convert into transform domain. The four sub bands viz., LL, HL, LH and HH of sizes 2*2 are obtained for DWT and IWT. For embedding process, the HH bands of DWT/IWT are considered. The HH coefficients of DWT are quantized to get integer values.

3.2.5. Modification**:** All the columns of payload pixel values are converted into single column. These pixels are converted in to binary. For hiding data, two payload bits (b_1, b_2) are considered at a time. In this technique, the MSB of all pixels are considered first for hiding. We can choose payload bits in any manner.

Consider the identity matrix I = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Modification matrix I_M is obtained from I using the conditions given below;

(a) If the both bit pair of payload are (0, 0) then there is no change in I.

$$I_M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

(b) If both bit pair of payload are (1, 1) then both rows of I are interchanged.

$$I_M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(c) If the bit pair of payload are (0, 1) then second row elements are interchanged.

$$I_M = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

(d) If the bit pair of payload are (1, 0) then first row elements are interchanged.

$$I_M = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$$

3.2.6. Multiplier: Multiply I_M with 2x2 HH sub band of cover image WT which results in stego matrix, I_M X = K

Let 2 * 2 cover image as X = $\begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix}$

Case (i): If the payload bit pair is (0, 0) then the stego-matrix is same as cover image matrix i.e,

$$K = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix} = \begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix}$$

Case (ii): If the payload bit pair is (0, 1), then K results in stego matrix in which both rows are identical and same as the first row of X.

$$K = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix} = \begin{bmatrix} 5 & 8 \\ 5 & 8 \end{bmatrix}$$

Case (iii): If the payload bit pair is (1, 0) then stego matrix will have both the rows same as the second row of X.

$$K = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix} = \begin{bmatrix} 6 & 9 \\ 6 & 9 \end{bmatrix}$$

Case (iv): If the payload bit pair is (1, 1) then the stego matrix will have second row of X as first row and first row of X as second row

$$K = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 5 & 8 \\ 6 & 9 \end{bmatrix} = \begin{bmatrix} 6 & 9 \\ 5 & 8 \end{bmatrix}$$

3.2.7. Key**:** It is used to extract the payload at the destination so that first bit of the payload bit pair is taken as reference in order to avoid unintended recipient.

3.2.8. Inverse Wavelet Transform: The 2*2 matrices are obtained from the Multiplier to form stego DWT/IWT matrices. Inverse DWT/IWT is applied to generate stego image in the spatial domain.

3.3. Payload Extraction

The retrieval of payload from stego image is given in the Figure 2.

3.3.1. Stego Image (SI): The image which contains secret image that has to be extracted.

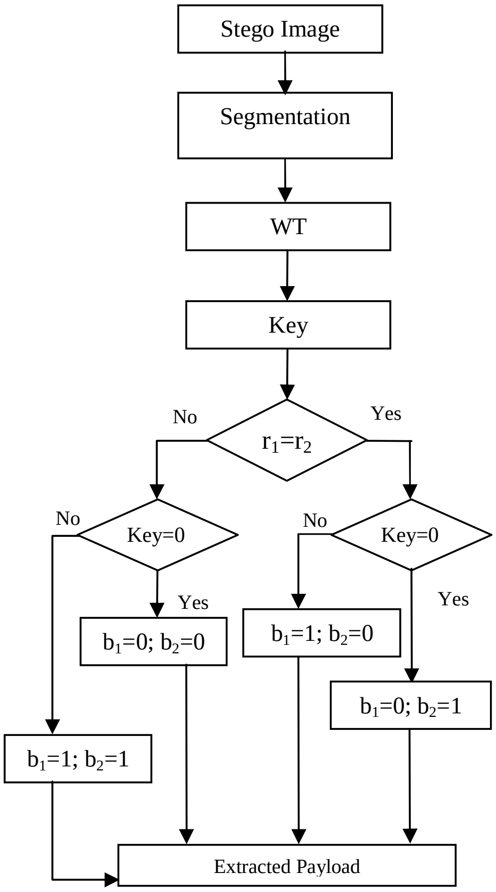


Figure 2. WNLS extraction system

3.3.2. Segmentation: The Stego image is decomposed into matrix of size 4*4

(3.3.3) Wavelet Transform (WT): The two dimensional DWT and IWT are applied on each 4*4 matrix of stego image to convert into transform domain. The four subbands viz., LL, HL, LH and HH are obtained for DWT and IWT. The HH coefficients of DWT are quantized to get integer values.

3.3.4. Key: Key plays an important role in order to extract the bits from each 2*2 stego image matrix block.

3.3.5. Matrix Comparison: (i) If first row (r_1) and second row (r_2) are same, two payload bit pairs are (0, 1) or (1, 0) be hidden. In order to know which payload bit pair is hidden we have to consider the first element of bit pair of the payload if it is 0, then embedded bits is (0, 1) otherwise (1, 0) and the extracted are also same. (ii) If first row (r_1) and second row (r_2) are different, two payload bit pairs (0, 0) or (1, 1) be hidden. In order to know which payload bit pair is hidden we have to consider the first element of bit pair if it is 0, then embedded bits is (0, 0) otherwise (1, 1) and the extracted are also same. Hence the element represents the key 0 or 1. All the extracted bits are arranged in an order to get embedded payload.

4. Algorithm of WNLS

Problem definition: The payload is embedded into the cover image using non-LSB technique. Cover Image is segmented and DWT/IWT is applied to generate 2*2 cells. The payload bit pairs are manipulated with 2*2 cells of DWT/IWT to generate stego object. The objectives are (i) To generate a stego image for secure communication.
(ii) To increase PSNR value between CI and SI.
(iii) To increase security level.
Assumption: Noiseless communication channel.

4.1. Embedding Algorithm

The embedding of payload using WNLS algorithm is given in table 1.

Table 1. WNLS Embedding Algorithm

Input: Cover image, Payload,
Output: Stego Image

1. Divide the cover image into blocks of size 4*4.
2. Apply Wavelet transform on each 4*4 matrix. Consider only HH sub band of size 2*2 bits.
3. If the rows of the block are identical, then change one of the elements;
4. Consider a bit pair (b_1, b_2) of payload and identity Matrix I.
5. If the first bit of payload bit pair is zero, then the first row of I is not changed; else the elements of the first row are interchanged in the I.
6. If the second bit of payload bit pair is zero, then the second row of I is not changed; else the elements of the second row are interchanged in the I.
7. The matrix I_M is multiplied with the 2*2 valid HH sub band of cover image block to get stego image block.
8. First bit of bit-pair is considered as key for payload extraction at the destination.

4.2. Extraction Algorithm

The payload is extracted from the stego image and WNLS algorithm is given in table 2.

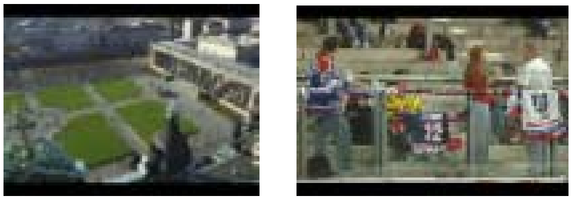
Table 2. WNLS Extraction Algorithm

```
Input: Stego image
Output: Payload
1.  Divide the stego image into blocks of size 4*4 blocks.
2.  Apply Wavelet Transform on each 4*4.
3.  Extract key from stego image.
4.  Access one block at a time.
5.  Access the key corresponding to that block.
6.  If the rows are not identical and the key is 0, then the bits
      extracted are (0, 0).
7.  If the rows are not identical and the key is 1, then the bits
      extracted are (1, 1).
8.  If the rows are identical and key is 0, the bits extracted are
      (0, 1).
9.  If the rows are identical and key is 1, the bits extracted are
      (1, 0).
10. Construct the payload with bits extracted
```

5. Performance Analysis and Results

Cover image of different sizes and formats viz., JPEG, BMP, TIFF, PNG and Raw images are considered for performance analysis. Steganography performance is analysis using PSNR. The few CI images Garden, Football fans, House and Water house are shown in Figure 3. The few PL images are Cups, Lion, Sony and Rose are shown in Figure 4. Table 3, 4, 5, 6 and 7 gives the PSNR values using IWT and DWT for cover image with stego image and payload with extracted payload for raw images, JPEG, BMP, TIFF and PNG respectively. It is observed that the value of PSNR between CI and SI is better in case of IWT compared to DWT in all image formats. The value of PSNR between PL and Extracted payload (EPL) is better in the case of DWT compared to IWT in all image formats.

Table 8 gives the PSNR between cover image and stego image for different image formats. It is observed that the PSNR is better using IWT in comparison with DWT for all image formats. The PSNR values are high in the case of raw images compared to formatted images. Since raw images has more redundant information. The proposed algorithm is robust since, it is non LSB technique and also transform domain. The security to the payload is high as the payload bits are not embedded into the cover image directly. The identification and estimation of payload bit length can’t be detected by standard stegagalysis techniques such as Chi-square [12] and pair of values [13].


(a) garden (b) football Fans (FF)

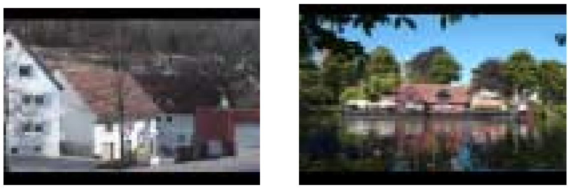
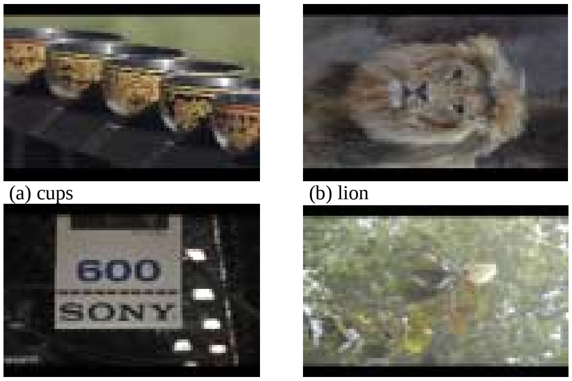

(c) house (d) water house (WH)

Figure 3. cover images


(a) cups (b) lion

(c) sony (d) rose

Fig ure 4. payload images

Table 3. PSNR using IWT and DWT for RAW images of WNLS.

Cover Image	Payload	IWT		DWT	
		CI and SI	PL and EPL	CI and SI	PL and EPL
*Garden 512*512*	Rose 64*64	50.395	27.44	45.780	27.199
*FF 640*640*	Cups 80*80	50.025	27.87	46.657	28.138
*House 720*720*	Lion 90*90	50.738	28.10	46.436	28.476
*WH 880*880*	Sony 110*110	52.224	27.74	47.765	28.044

Table 4. PSNR using IWT and DWT for JPEG images of WNLS.

Cover Image	Payload	IWT		DWT	
		CI and SI	PL and EPL	CI and SI	PL and EPL
Garden 512*512	Rose 64*64	33.67	27.21	33.49	27.20
FF 640*640	Cups 80*80	38.21	26.73	37.82	26.75
House 720*720	Lion 90*90	31.36	29.08	31.26	29.08
WH 880*880	Sony 110*110	33.76	29.59	33.64	29.59

Table 5. PSNR using IWT and DWT for BMP images of WNLS.

Cover Image	Payload	IWT		DWT	
		CI and SI	PL and EPL	CI and SI	PL and EPL
Garden 512*512	Rose 64*64	33.67	27.22	33.49	27.21
FF 640*640	Cups 80*80	38.21	26.71	37.81	26.75
House 720*720	Lion 90*90	31.36	29.08	31.26	29.08
WH 880*880	Sony 110*110	33.75	29.59	33.64	29.59

Table 6. PSNR using IWT and DWT for TIFF images of WNLS.

Cover Image	Payload	IWT		DWT	
		CI and SI	PL and EPL	CI and SI	PL and EPL
Garden 512*512	Rose 64*64	33.67	27.22	33.49	27.21
FF 640*640	Cups 80*80	38.21	26.71	37.81	26.75
House 720*720	Lion 90*90	31.36	29.08	31.26	29.08
WH 880*880	Sony 110*110	33.75	29.59	33.64	29.59

Table 7. PSNR using IWT and DWT for PNG images of WNLS.

Cover Image	Payload	IWT		DWT	
		CI and SI	PL and EPL	CI and SI	PL and EPL
Garden 512*512	Rose 64*64	33.67	27.22	33.49	27.21
FF 640*640	Cups 80*80	38.21	26.71	37.81	26.75
House 720*720	Lion 90*90	31.36	29.08	31.26	29.08
WH 880*880	Sony 110*110	33.75	29.59	33.64	29.59

References

[1] Souvik Bhattacharyya and Gautam Sanyal, A Data Hiding Model with High Security Features Combining Finite State Machines and PMM method, International Journal of Electrical and Computer Engineering, 5(2), 2010,78-85.

[2] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal, A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method, International Journal of Computer science and Information security, 4(2), 2010, 96-103.

[3] Hongmei Tang, Gaochan Jin, Cuixia Wu and Peijiao Song, A New Image Encryption and Steganography Scheme, IEEE International Conference on Computer and Communications Security,2009, 60-63.

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

Table 8. PSNR between CI and SI for different image formats of proposed WNLS algorithms.

Cover Image	Payload	PSNR									
		RAW Images		JPEG		BMP		PNG		TIFF	
		IWT	DWT	IWT	DWT	IWT	DWT	IWT	DWT	IWT	DWT
Garden 512*512	Rose 64*64	50.395	45.780	33.677	33.499	33.675	33.498	33.675	33.498	33.675	33.498
FF 640*640	Cups 80*80	50.025	46.657	38.219	37.820	38.217	37.818	38.217	37.818	38.217	37.818
House 720*720	Lion 90*90	50.738	46.436	31.368	31.262	31.368	31.262	31.368	31.262	31.368	31.262
WH 880*880	Sony 110*110	52.224	47.765	33.764	33.649	33.758	33.644	33.758	33.644	33.758	33.644

6. Conclusions

Steganography is the technique of hiding information in digital media in order to conceal the existence of the information. In this paper WNLS algorithm is proposed. The cover image is segmented into 4*4 matrices. The DWT/IWT is applied on each cell to derive sub bands. The Payload bit pairs are manipulated with 2*2 bands of DWT /IWT to derive stego image. It is observed that PSNR value is better in the case of IWT compare to DWT. The proposed algorithm is robust since the payload is embedded into the transform cover image indirectly.

In future the algorithm can be tested with some more transform domain techniques to improve the performance.

Acknowledgements

The first author would like to thank the Principal Dr Narendra Viswanath, and HOD(ECE) Prof. K N Ramachandra Rao and the Management of Global Academy of Technology, Bangalore for their continuous support to pursue this research work.

[5] Nedal M S Kafri and Hani Y Suleiman, Bit-4 of Frequency Domain-DCT Steganography Technique, IEEE International Conference on Networked Digital Technologies, 2009, 286-291.

[6] Han Ling Zhang, Guang Zhi Geng and Cai Qiong Xiong, Image Steganography using Pixel Value Differencing, IEEE International Symposium on Electronic Commerce and Security, 2009, 109-112.

[7] Saeed Sarreshtedari, Mohsen Ghotbi and Shahrokh Ghaemmaghami, One Third Probability Embedding: Less Detectable LSB Steganography, IEEE International Conference on Multimedia and Expo, 2009, 1002-1005.

[8] Ravuru Rakesh, Shantan Devathi, Prashanth Sekhar and Chandra Sekaran, Adaptive Randomization in Image Steganography Pertaining to Most Significant Nibble, International Journal of Computer Applications,22,2011, 1-6.

[9] Dipti Kapoor Sarmah and Neha Bajpai , Proposed System for Data Hiding Using Cryptography and Steganography, International Journal of Computer Applications, 8(9), 2010, 7-10.

[10] P. T. Anitha, M. Rajaram and S. N. Sivanandham, Analysis of Detecting Steganography contents in corporate Emails, International Journal of Research and Reviews in Electrical and Computer Engineering,1(2), 2011, 92-97.

[11] Manjunath Gadiparthi, Keshav Sagar and Divya Sahukari, A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods, International Journal of Computer Applications, 22(5), 2011, 8-11.

[12] Chiew Kang Leng, Jane Labadin and Sarah Flora Samson Juan, Steganography: DCT Coefficients Reparation Technique in JPEG Image, International Journal of Digital Content Technology and its Applications, 2(2), 2008, 35-41.

[13] Raja K B, Rohitha L. Rekha S, Swetha P V, Venugopal K R and Patnaik L M , LSB steganalysis to detect embedded message length using pixel pair threshold, International conference on Advanced Computing and Communications, 2007, 765-770.

Authors Biography

H S Manjunatha Reddy is a Professor in the department of Electronics and Communication Engineering, Global Academy of Technology, Bangalore. He obtained his B.E. Degree in Electronics from Bangalore University, Bangalore. His specialization in Master degree was Digital Electronics from Visvesvaraya Technological University, Belgaum. He is pursuing research in the area of Steganography and Steganalysis for secured communication. His area of interest is in the field of Digital Image Processing, Communication Networks and Biometrics. He is life member of ISTE, New Delhi.

K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering and Master of Engineering in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 75 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing and computer networks.