Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Adaptive Image Steganography Based on Denoising Methods in IWT

[1]G. Prabakaran [2]R. Bhavani [3]M. Kiruthika*
[1] Assistant Professor, Dept. of CSE, Annamalai University, Annamalai Nagar, Tamil Nadu, India
[2]Professor, Dept. of CSE, Annamalai University, Annamalai Nagar, Tamil Nadu, India
[3]PG Student, Dept. of CSE, Annamalai University, Annamalai Nagar, Tamil Nadu, India

Abstract: ***The Steganography is used for secure communication of information by embedding information in a cover object such as text, image, audio, video without any suspicion. An adaptive image steganography utilizing image denoising algorithm by wavelet thresholding. Adaptive steganography is a spatial case of both spatial and transform technique. Moreover it is introduced as statistics aware embedding and masking. Wavelet transform is employed to represent represent spatial domain image into time frequency domain. At first Arnold Transformation is performed to scramble the secret message then both cover and secret message are decomposed using Integer wavelet transform. In general secret data is hidden in noisy components of cover medium, this implies that calculating a threshold based on wavelet coefficients of cover image to determine the noisy components. Afterwards the decomposed secret message embedded among noisy coefficients. This proposed method improves the capacity, Peak Signal to Noise Ratio (PSNR) and provides high security and certain robustness.***

Keywords: Adaptive Steganography, Denoising Methods, IWT, Arnold Transformation, Image quality Metrics.

I. INTRODUCTION

With the recent advances in multimedia communications and its influence in our electronic world, the importance of information security has been dramatically increased. Existing technologies in the field of information security systems offer concealing the occurrence of communication for anyone except the intended recipient. In this way, steganography provides a reliable solution for embedding a secrete data into a cover media imperceptibly. Basically, the ultimate objectives of steganography are undetectability, robustness, and high capacity of the hidden data that separate it from related techniques such as watermarking and cryptography. Also, the hidden message can be recovered using appropriate keys without any knowledge of the original cover media. In general, steganography algorithms usually struggle with achieving a high embedding rate, large capacity, and good imperceptibility. There are many applications that exploit the ability of steganography to hide secret message in the form of text, imaginary, or any other digital signal. Applications for such a data-hiding scheme include in-band captioning, covert communication, image tamper proofing, revision tracking, and enhancing robustness of image search engines. This work aims to present an efficient steganography technique in image files. The most common steganographic techniques in digital images focus on spatial domain methods-which generally use a direct Least Significant Bit (LSB) replacement technique- and frequency domain methods such as Discrete Cosine Transform (DCT), Fourier Transform (FT), and Discrete Wavelet Transform (DWT).

II. RELATED WORK

Atallah M. Al-Shatnawi [1] has proposed a method for hiding the secret message based on searching about the identical bits between the secret messages and image pixels values. The proposed method is compared with the LSB benchmarking method. The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. The proposed method is efficient, simple and fast it robust to attack and improve the image quality, hence it obtained an accuracy ratio of 83%.

M. Ravi Shankar Reddy & Sri. J. Swami Naik [2] have proposed a technique for the hiding of text messages into a digital image in spatial domain. In our approach in each pixel two bits of message part is embedded in such a way that the fourth bit place, second bit plane and also the least significant bits are allowed. Proposed message hiding approach is robust and very useful in real world applications.

Weiqi Luo et al., [3] have proposed an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. The proposed method enhances the security as well as preserving higher visual quality of stego images.

Yambem Jina Chanu et al., [4] have proposed an Adaptive Stegnographic technique, which embeds secret message bits in the edges of the images is proposed.

Fatema Akhter et al., [5] have proposed a new approach for information hiding in digital image in spatial domain by selecting three bits of message is embedded in a pixel using Lucas Number system but only one bit allowed

for alternation. Proposed method has the larger capacity of embedding data, high peak signal to noise ratio compared to existing methods and is hardly detectable for steganolysis algorithm.

Chao Wang et al., [6] proposed a method to increase the embedding speed of matrix embedding by extending the matrix via some referential columns. Compared with the original matrix embedding, the proposed method can exponentially reduce the computational complexity for equal increment of embedding efficiency. Proposed method achieves higher embedding efficiency and faster embedding speed than previous fast matrix embedding methods.

N Sathisha et al., [7] have proposed Non Embedding Steganography using Average Technique in Transform domain (NESATT). The Lifting Wavelet Transform (LWT) is applied on both cover image and payload image. The Diagonal band (CD) of cover image and Approximation band (PA) of payload are segmented into N x N blocks. The PA band of payload is divided by CD to generate resultant matrix based on Non Embedding Threshold Value (NETV) fixed by key. The average value of resultant matrix is calculated and used to divide PA to generate modified CD. The average value of each blocks are scale downed by key and embedded into corresponding block of Horizontal band (CH) of cover image. The inverse LWT is applied on stego object. The capacity and PSNR values are high in the case of proposed algorithm

A.Antony Judice et al., [8] have proposed a novel technique 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 (OPA) algorithm. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic system.

Ali Al-Ataby & Fawzi Al-Naima [9] have proposed a method that pre-adjusts the original cover 1image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered. Then, it uses Wavelet transform to transform both the cover image and the hidden message. The proposed technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security.

Ashish Chawla & Pranjal Shukla [10] have proposed a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Matrix Rotation is performed to scrambles the secret image. Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is
applied to get the stego image. Proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility.

H.S. Manjunatha Reddy & K.B. Raja [11] have proposed a Wavelet based Non LSB Steganography (WNLS) in which the cover image is segmented into 4 x 4 cells and DWT/IWT is applied on each cell. The 2 x 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. PSNR Rate is high for this proposed system.

Tao Ran Zheng Zhou & Zhang Tao Zheng Zhou [12] have proposed a data hiding algorithm in which, the image is decomposed into blocks, after which the texture complexity of each block is calculated and blocks with high complexity are selected. Then the different pixel values on two directions of the selected blocks are computed to choose the edge areas. The secret messages are only embedded in the pixel-value differencing above the threshold. The experimental results show that our method outperforms previous steganographic methods such as LSB matching and Adaptive data hiding in edge areas of images on the capability of resisting universal blind detecting methods, such as wavelet high-order statistics analysis.

S.Jayasudha [13] has proposed a data hiding scheme hide secret data in a random order using a secret key only known to both sender and receiver. In this method, embeds different number of bits in each wavelet co efficient according to a hiding capacity function in order to increasing the hiding capacity without losses of the visual quality of resulting stego image.

Manisha Boora & Monika Gambhir [14] have proposed a scheme for hiding a larger size secret-image into smaller size cover- image. Arnold Transformation is performed to obtain scrambled secret image. DWT is performed on both cover image and secret image and this is followed by alpha blending operation. This proposed algorithm is highly secured with good perceptual invisibility.

Minati Mishra et al., [15] have proposed a technique that uses spatial domain LSB substitution method for information embedding and Arnold's transform is applied twice in two different phases to ensure security. The proposed method is highly secure and provides high data hiding capacity.

III. METHODOLOGY

A. PRE-PROCESSING

Histograms are functions describing information extracted from the image. The histogram function is defined over all possible intensity levels. For each intensity level, its value is equal to the number of the
pixels with that intensity. Adaptive histogram equalization uses the histogram equalization mapping function supported over a certain size of a local window to determine each enhanced density value. Therefore regions occupying different gray scale ranges can be enhanced simultaneously.

B. INTEGER WAVELET TRANSFORM (IWT)

In this proposed paper, Haar integer wavelet transform is applied to the cover image for embedding the secret data bits .The first level IWT will result the high (H) and low (L) frequency wavelet coefficients of the cover image. High

frequency wavelet coefficients are obtained by taking the edge information between the adjacent pixel values and low frequency wavelet coefficients are obtained by suppressing the edge information in each pixel value.

First Level IWT:

$$H = Cz - Ce \quad (1)$$

$$L = Ce - [H/2] \quad (2)$$

Where, Co and Ce is the odd column and even column wise pixel values. The H and L bands of the first level IWT are passed through the second level of high pass and low pass filter banks to get the IWT coefficients, which contains LL, LH, HL, HH bands, where the LL band contains highly sensitive information of the cover image. The other 3 bands LH, HL and HH contain the detailed information of the cover image.

Second Level IWT:

$$LH = Lodd - Leven \quad (3)$$

$$LL = Leven - [LH / 2] \quad (4)$$

$$L = Hodd - Heven \quad (5)$$

$$HH = Heven - [H\ L/\ 2] \quad (6)$$

Where, Hodd is an odd row of H band, Lodd is an odd row of L band, Heaven is even row of H band and live-in is even row of L band. As IWT is reversible transformation. the image is reconstructed by applying inverse integer wavelet transform to the LL, LH, HL and HH bands.

C. ARNOLD TRANSFORM

Arnold Transform is commonly known as Cat face Transform and is only suitable for N×N images digital images. It is defined as

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \quad (7)$$

Where (x, y) are the coordinates of original image, and (x',y') are the coordinates of image pixels of the transformed image. Transform changes the position of pixels and if done several times, scrambled image is obtained. N is the height or width of the square image to be processed. Arnold Transform is periodic in nature. The decryption of image depends on transformation periods. Period changes in accordance with size of image. Iteration number is used as the encryption key. When Arnold Transformation is applied, the image can do iteration, iteration number is used as a secret key for extracting the secret image.

D. GENERIC BLIND IMAGE STEGANOGRAPHIC SYSTEM

A message is embedded in a digital image by the embedding function, which uses a key or password. The resulting stego-image is transmitted over a channel to the recipient, where it is processed by the extracting function using the same key. During transmission, the stego image can be monitored by unintended viewers who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message.

The parameters of steganographic system, such as the number of data bits that can be hidden, the invisibility of the message, and its resistance to removal, can be related to the characteristics of communication systems such as capacity and Peak Signal-to-Noise Ratio (PSNR). The notion of capacity in data hiding indicates the maximum number of bits hidden and successfully recovered by the stego systems. In our study, it refers to the ratio of maximum number of DWT coefficients of cover image which is replaced by DWT coefficients of secret image. The PSNR serves as a measure of invisibility, or detectability.

E. THRESHOLD SELECTION BASED ON DENOISING METHODS

The selection of threshold calculation method is the main issue of wavelet threshold denoising in the proposed method. Generally calculation of the threshold is done via statistical means in image denoising. It can be solved using two basic approaches, spatial filtering methods and transform domain filtering methods. Spatial Filtering is a simple way to remove noise from image data which uses a fixed or adaptive threshold to recover the corruption of noise in digital image acquisition and transmission phase. On the other hand, a vast literature has emerged recently on image denoising via wavelet thresholding or shrinkage that is firstly introduced by Donoho and Johnstone. They presented a method named wavelet shrinkage to overcome the weaknesses of the spatial filtering, and showed its obvious efficiency on signal denoising and inverse problem solving. It's the primer work in transform domain. In this method, a DWT is performed on the noisy signal. Then with a preset threshold, coefficients with magnitude smaller than the threshold are set to zero while those with larger magnitude are kept and used to estimate the noiseless coefficients. Finally, an inverse DWT (IDWT) reconstructs the signal from the estimated coefficients. Based on Donoho report, σ is estimated using detail coefficient of wavelet transform as in equation (8).

$$\sigma = 1/0.6545(\ median(\ |c|\ ))\quad (8)$$

where c is the detail coefficients of wavelet transform. Imagine n_c as the number of all the wavelet coefficients and c_{fs} as content all the wavelet coefficients.

Donoho universal method threshold as follow as in equation (9)

$$T_{Donoho} = \sigma \sqrt{(2 \log(N))} \quad (9)$$

Where, *N* is the size of considered wavelet coefficients.

As a Matlab toolbox function *Minimax* threshold uses a fixed threshold chosen to yield minimax performance for mean square error against an ideal procedure. The minimax principle is used in statistics in order to design estimators. Since the denoised signal can be assimilated to the estimator of the unknown regression function, the minimax estimator is the one that realizes the minimum of the maximum mean square error given in equation (10)

$$T_{minimax=}0.3936+ 0.1829(\log(N)/\log(2)) \quad (10)$$

The above described threshold calculation methods are considered in the study as a modification to improve parameters of steganographic system.

F. THE PROPOSED EMBEDDING METHOD

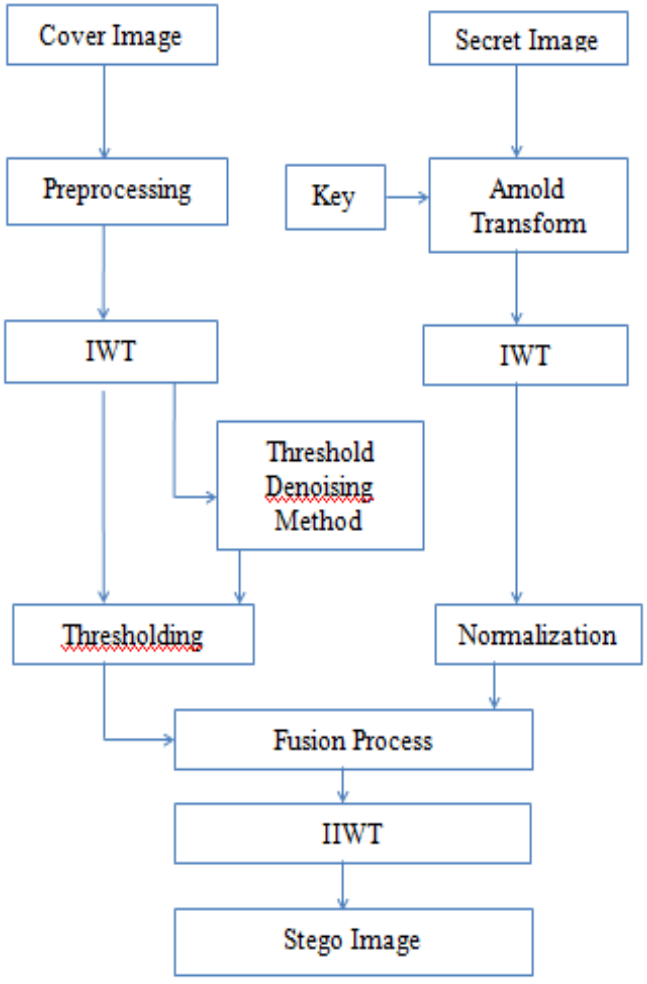
The fundamental concept of proposed method is the embedding of the hidden information within noise data of an image, which is originally, spreads over cover image. Generally, approximation coefficients of wavelet transform have no noisy pattern and are not suitable for embedding because they carry the most information content of the whole cover image. Therefore, details coefficient are the most convenient noisy area for embedding a secret data. Block diagram of the proposed steganography system is depicted in Figure (1) below. According to this figure, the process of the embedding and extracting the secret data can be described as follow:

Algorithm for Embedding Process:

- Input: Cover Image, Secret Image
- Output: Stego Image

Step 1: Preprocessing the cover Image
Step 2: Arnold Transformation with key takes place to scramble the secret message.
Step 3: 2D IWT Transformation takes place on both cover image and secret message.
Step 4: Threshold calculation using denoising method using 2D IWT coefficients of cover Image.
Step 5: Normalize the IWT coefficients of message to threshold
Step 6: Replacing threshold IWT coefficients of cover image with normalized IWT coefficients of message.
Step 7: Finally, Inverse IWT can takes place to form the Stego Image.

Embedding Process:



Extracting Process:

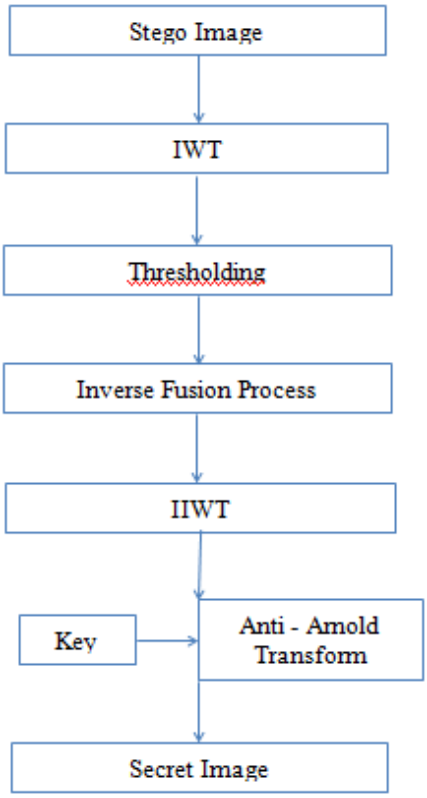


Fig.1 Block diagram of Proposed Method.

Algorithm for Extracting Process:

- Input: Stego Image
- Output: Secret Image

Step 1: 2-D IWT Transformation
Step 2: Threshold will be calculated using denoising method using 2-D IWT coefficients of Stego Image
Step 3: Normalize the IWT coefficients of message to threshold
Step 4: Inverse fusion process
Step 5: Inverse IWT Transformation
Step 6: Arnold Transformation with same key on Embedding takes place to reconstruct the original Image.
Step 7: Secrete Image formation.

IV. RESULTS AND DISSCUSSION

Four Images with different characteristics are used to examine the performances of the proposed steganoraphy system. The original 300x300 images appear in Figure.2. and are entitled Winter, Water lilies, Sunset and Lavender respectively. In the following procedure, the source image is decomposed into two levels of IWT for accessing to noise components. Fig. 3 shows the proposed method applied to cover image of size 300x300 and Secret image or payload of size 150x150. Figure 3.(b) is the corresponding Histogram of Cover image, figure 3.(d) is the Stego image and corresponding Histogram shown in figure 3.(e). The final recoverd image is shown in figure 3.(f).

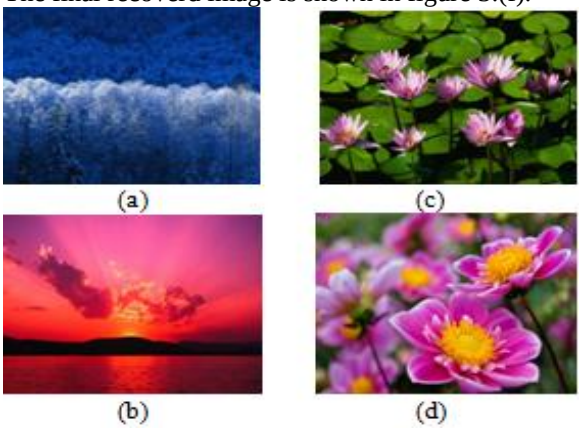


Fig. 2. Basic test images for Steganography (a). Winter, (b).Sunset, (c).Water Lillies and (d).Lavender.

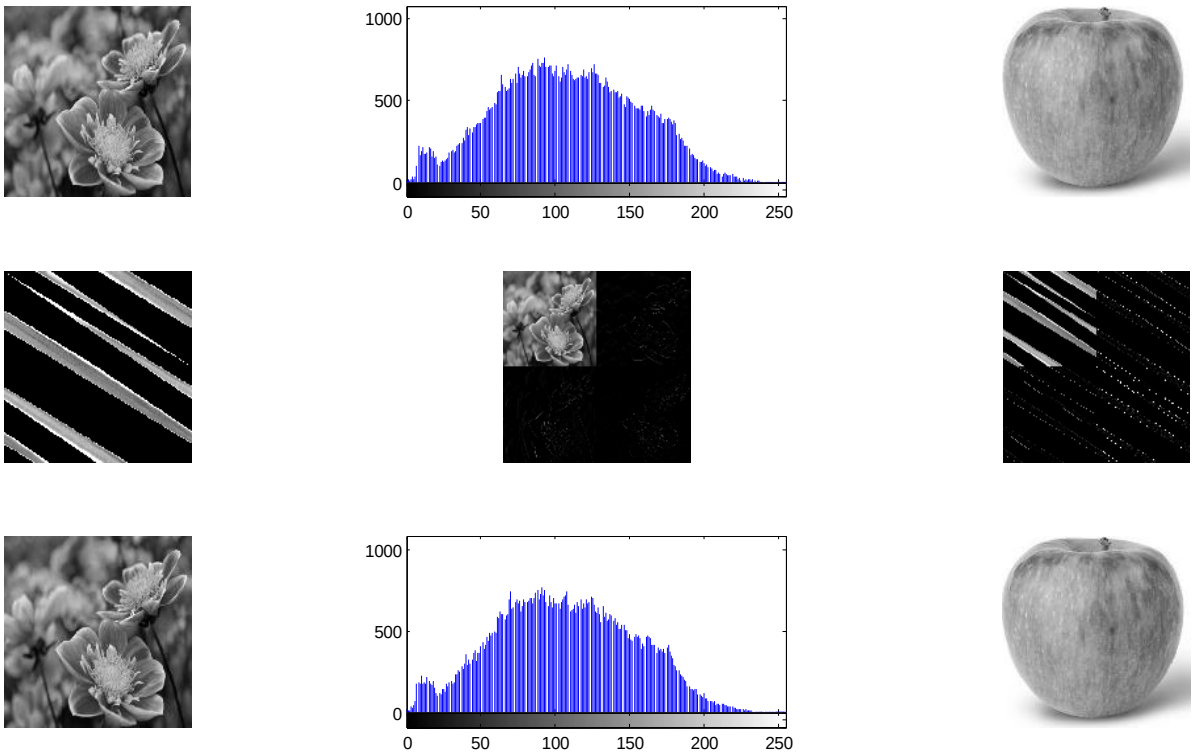


Figure 3. Experimental result for IWT (a) Cover image, (b) Histogram of cover image, (c) Secret image, (d) Arnold Transform, (e) Cover dwt , (f) Secret dwt , (g) Stego image , (h) Histogram of stego image, (i) Original image

Table .1 Performance of proposed method for different cover and secret images

Cover	Secret	MSE	PSNR	NCC	AD	SC	MD	NAE
Winter	Sunflower2	2.99	43.38	0.98	1.29	1.04	5.94	0.02
Water lilies	Sunflower2	3.59	42.57	0.98	1.48	1.04	6.97	0.02
Sunset	Sunflower2	4.32	41.78	0.98	1.75	1.04	5.97	0.02
Lavender	Sunflower2	5.27	40.91	0.98	1.97	1.04	6.97	0.02
Winter	Apple3	2.82	43.63	0.98	1.19	1.04	5.94	0.02
Water lilies	Apple3	3.37	42.85	0.98	1.37	1.03	6.97	0.02
Sunset	Apple3	4.07	42.03	0.98	1.67	1.03	5.97	0.02
Lavender	Apple3	4.98	41.16	0.98	1.88	1.03	6.97	0.02

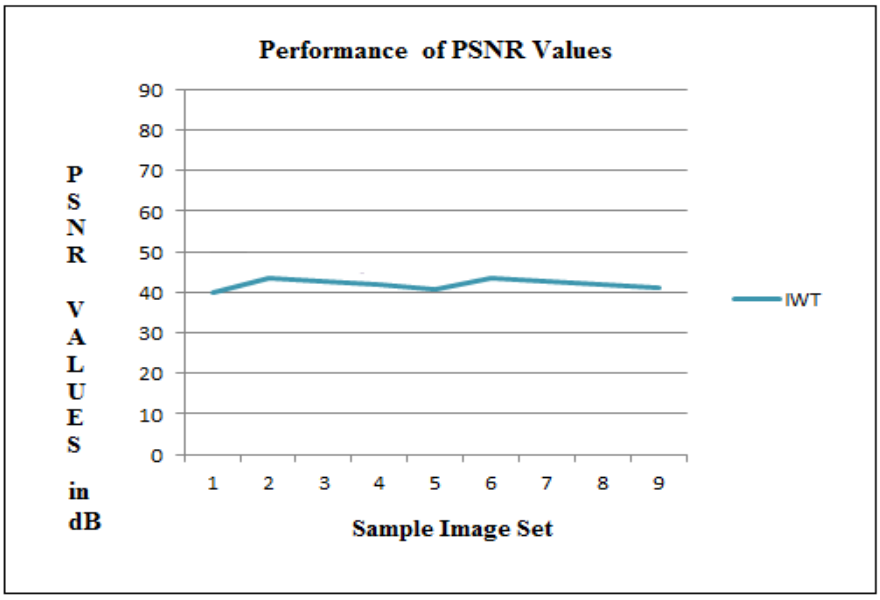


Figure 4.The PSNR vs Sample Image Set

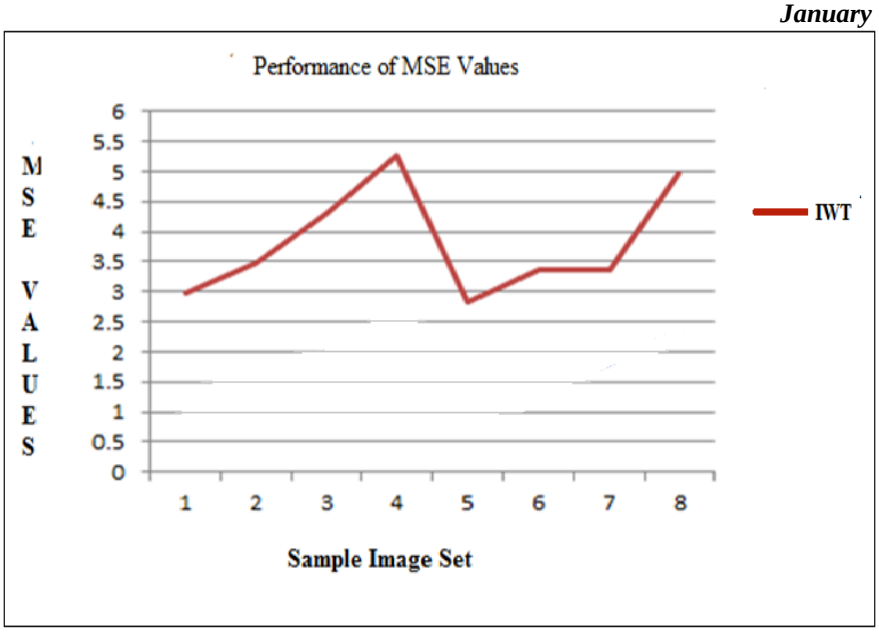


Figure 5.The MSE vs Ssample Image Set

From Table 1 various Image Quality metrics like Mean square Error (MSE), Peak signal to Noise Ratio (PSNR), Normalized Cross Correlation (NCC), Average Difference (AD), Structural Content (SC), Maximum Difference (MD), and Normalized Absolute Error (NAE) values are illustrated with various Cover images and Secret Images. It illustrates that the value are MSE lies between 2.82 to 5.27, PSNR lies between 40.9 to 43.6, NCC values lies in the range from 0 to1, AD values is in between 1.19 to 1.97, SC lies between 1.03 to 1.04, MD values lies in the range from 5.94 to 6.97 and NAE lies between 0.0 to 0.02.

The performance of PSNR values versus sample image sets shown in the Line graph. The results of all the method versus one set of the image. Figure 4. shows the excellent performance ratio values in IWT. The performance of MSE values versus sample image sets shown in the Line graph. The results of all the method versus one set of the image. Figure 5. shows the excellent performance ratio values in IWT.

V. CONCLUSION

We have presented a novel steganographic methodology that utilizes 2D wavelet transform and image denoising techniques. This process provides a method for concealing a digital data within a cover image by adjusting a threshold value from denoising methods to propose a high payload (capacity) with very little effect on statistical properties. In this steganography system both cover image and secret data are decomposed into 2 level of wavelet decomposition. By applying a threshold which is calculated from detail coefficients of cover image, embedding points are detected and filled by normalized DWT coefficients of secret message. Experimental results shows that this proposed system gives the high security and capacity. As future extension, we would like to enhancing capacity and PSNR rate by level dependent denoising methods.

REFERENCE

[1] Atallah M. Al-Shatnawi, 2012, ”A New Method in Image Steganography with Improved Image Quality”, Applied Mathematical Sciences, vol 6, pp 3907-3915.

[2] M. Ravi Shankar Reddy et al., 2013, “A Novel Method for Steganography in Spatial Domain”,International Journal of Advanced Research in computer Science and Software Engineering, vol 3, issue 10.

[3] Weiqi Luo & Jiwu Huang, 2010, “Edge Adaptive Image Steganography Based on LSB Matching Revisited”, IEEE Transaction on Information Forensics and Security , vol 5, no 2, pp 201-214.

[4] Yambem Jina Chanu et al., 2014, “Adaptive Edge Stegnography for Images”, International Journal of Information and Computation Technology, vol 4, no 7, pp 777-786.

[5] Fatema Akhter et al., 2013 “A Novel Approach for Image Steganography in Spatial Domain”, Global Science of computer Science and Technology Graphics & Vision, vol 13,issue 7, ver 1.0, pp 1-6.

[6] Chao Wang et al., 2012, “Fast Matrix Embedding by Matrix Extending”, IEEE Transactions on Information Forensics and Security, vol 7, pp 346-350.

[7] N Sathisha et al., 2013, ”Non Embedding Steganography using Average Technique in Transform Domain”, IEEE 9th International Colloquium on Signal processing and its Applications, pp 1-6.

[8] A.Antony Judice et al., 2014, “An Image High Capacity Steganographic Methods by Modified OPA Algorithm and Haar Wavelet Transform”,IJCSNS International Journal of computer Science and Network Security, vol 14, pp 125-132.

[9] Ali Al-Ataby & Fawzi Al-Naima, 2010, ”A Modified High Capacity Image Steganography Technique Based on Wavelet Transform”, The International Arab Journal of Information Technology, vol 7, pp 358-364.

[10] Ashish Chawla & Pranjal Shukla, 2013, "A Modified Secure Digital Image Steganography based on Dwt using Matrix Rotation Method", International Journal of Computer Science and communication Engineering, vol 2, pp 20-25.

[11] H S Manjunatha Reddy & K B Raja, 2011," Wavelet based Non LSB Steganography", International Journal of Advanced Networking and applications, vol 3,issue 3, pp 1203-1209.

[12] Tao Ran ZhengZhou & Zhang Tao ZhengZhou, 2012, "A Blind Detection Resistant Steganographic Algorithm for Images Based on Texture Complexity and Pixel-value Differencing", The 2nd International Conference on Computer Application and System and Modeling, pp 1240-1243.

[13] S.Jayasudha, 2013, "Integer Wavelet Transform Based Steganographic Method Using Opa Algorithm", International Journal of Engineering and Science, vol 2, issue 4, pp 31-35.

[14] Manisha Boora & Monika Gambhir, 2013, "Arnold Transform Based Steganography ",International Journal of Soft Computing and Engineering, vol 3, issue 4, pp 136-140.

[15] Minati Mishra et al., 2012, "High Security Image Steganography with Modified Arnold's Cat Map", International Journal of Computer Applications, vol 37, no 9, pp 16-20.

