# Eliminating Cover Image Requirement in Discrete Wavelet Transform based Digital Image Steganography

Parul Sehgal
M.Tech (p), Rajasthan Institute of Engineering & Technology, Jaipur, India.

Vijay Kumar Sharma
Assistant Professor, CS Deptt., Rajasthan Institute of Engineering & Technology, Jaipur, India.

## ABSTRACT
Image steganography is the art and science of hiding secret image into digital media such that no one apart from the intended recipient is able to detect the existence of the information. There are many different carriers that can be used to hide the information such as digital images, videos, sound files and other computer files but digital images are the most popular. In this paper, a method has been proposed using which a large size secret image can be hidden into small size cover image securely. The main aim here is the absolute invisibility of the large size secret image. The secret image is first scrambled by using Arnold transformation. Haar Discrete Wavelet Transformation (DWT) is then applied on cover image and Arnold transformed secret image, followed by Alpha Blending operation. Then the Haar Inverse Discrete Wavelet Transformation (IDWT) is applied to obtain the stego image. At the receiver side, first the cover image is obtained from the stego image. Then Haar DWT is applied on the cover image and the stego image followed by the alpha blending operation. Haar IDWT is applied on the resulting image. Then by applying Arnold transformation, the secret image is obtained. The proposed method does not require the sender to send the cover image to the receiver for obtaining the secret image. The performance of the proposed method is investigated by comparing the cover image and the stego image in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Normalized Cross Correlation (NCC). Experimental results demonstrate the effectiveness and accuracy of the proposed method.

## General Terms
Steganography, Arnold Transformation, Haar DWT, Haar IDWT, Alpha Blending, Adaptive Thresholding.

## 1. INTRODUCTION
Today, computers and internet have become the most powerful source of communication among the people in the different parts of the world. Long distances between the people are no longer an obstacle to exchange data between them. However, the safety and security of the exchanged data is of great concern, particularly in the case if it is confidential. The need to solve this problem led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security by the hidden exchange of information [4]. Steganography is derived from the Greek word steganos which means "covered" and graphy which means "writing" [3] [7].

Steganography's ultimate objectives and the main factors separate it from the related techniques such as cryptography and watermarking. Cryptography tends to modify the data into a form that an eavesdropper cannot understand. On the other hand, steganography tends to hide the existence of the message itself, which makes it difficult for an observer to find out where the message is [13]. Sometimes, sending encrypted information may draw the attention of an observer, while invisible information will not. Watermarking is similar, but has a completely different purpose. Watermarking is the process of embedding a message on the multimedia data. Placing a watermark in an image or other media file serves to identify the artist or author of the work i.e. it is used for copyright protection [9]. It is not so much an attempt to hide a message as it is to tag a document for later identification. A watermark can be either visible or invisible.

In recent years, the wavelet transform has emerged in the field of image processing as an alternative to the well-known Fourier Transform and its related transforms [10]. Formally, the wavelet transform is defined as a mathematical technique in which a particular signal is analyzed (or synthesized) in the time domain by using different versions of a dilated (or contracted) and translated (or shifted) basis function called the wavelet prototype or the mother wavelet. Wavelet transforms are now being adopted for a vast number of applications, e.g. internet, color facsimile, printing, scanning, digital photography, remote sensing, mobile applications, medical imagery, digital library, military applications and e-commerce. The wavelet transform is an upcoming technology within the field of image compression. Wavelet based coding provides significant improvements in picture quality at higher compression ratios.

## 2. RELATED WORK
Prabakaran.G and Bhavani.R [1] proposed a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. P.Chen, et al., [2] have proposed that a secret image is embedded into the high frequency coefficients resulting from Discrete Wavelet Transform while leaving the coefficients in the low frequency sub-band unaltered. H S Manjunatha Reddy, et al., [3] have proposed a high capacity and security steganography using Discrete Wavelet Transform in which the wavelet coefficients of both the cover and the payload are fused into single image using embedding strength parameters alpha and beta.

Nagham Hamid, et al., [4] proposed the various techniques of image steganography and presented the taxonomy of current steganography techniques for image files. Narasimmalou, T., et al., [5] proposed an optimal Discrete Wavelet Transform based steganography in which a single level DWT decomposition is done on a host image and the secret information is hidden by manipulating the transform coefficients of the decomposed image. Raja.K.B, et al., [6] have proposed a novel image adaptive steganographic technique in integer wavelet transform domain.

Babita Ahuja, et al., [7] proposed for more hiding capacity achieved by Filter Based scheme in Steganography. Tanmay Bhattacharya, et al., [8] proposed that two secret images are embedded within the HL and HH sub-bands of the DWT decomposed cover image and during embedding secret images are dispersed within each band using a pseudo random sequence and a session key. Nikita Kashyap, et al., [9] proposed a robust image watermarking technique for the copyright protection based on 3-level discrete wavelet transform, in which a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique.

M. Sifuzzaman, et al., [10] proposed that wavelet transform of a function is the improved version of Fourier transform and gave the advantages of wavelet transform compared to Fourier transform. Amitava Nag, et al., [11] proposed a novel technique for image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain and Huffman encoding is performed on the secret messages/image before embedding. Arash Vosoughi, et al., [12] proposed the use of discrete wavelet transform and Wiener filter for speckle noise suppression of ultrasound images. Shikha Sharda, et al., [13] proposed the important methods of steganography and presented the review of steganography in digital images.

This paper presents a new steganography method for embedding secret image into cover image with enhanced security. The main aim here is, firstly, the perfect invisibility of the secret message in the cover image, and secondly, the receiver should not require the sender to send the cover image for the decoding of the secret image.

The remaining chapters of the paper will be organized as follows: chapter three discusses about the proposed work, Arnold transformation, Discrete Wavelet Transform, Alpha Blending and implementation of the new proposed steganography method. Chapter four discusses the experimental results and analysis of proposed method. Chapter five gives the conclusion of the paper.

# 3. OVERVIEW OF PROPOSED WORK

The new proposed method consists of two processes- the encoding process and the decoding process. In encoding process, first apply Arnold transformation with security key on the secret image to get the scrambled secret image. This transformation gives more security and robustness to our new proposed method. Then apply Haar Discrete Wavelet Transform (DWT) on the Arnold scrambled secret image and the cover image in order to increase the security level. The alpha blending matrix is obtained by the addition of wavelet coefficients of respective sub-bands of cover image and Arnold scrambled secret image. Alpha factor is increasing the embedding strength factor. After the Alpha Blending operation, apply the Haar Inverse Discrete Wavelet Transform (IDWT) to get the stego image. The decoding process is the reverse of the encoding process.

The decoding process involves two steps. In the first step, take the logarithmic transform of the stego image. This log-transformed observation is separated in two images using Wiener filter, each of which is decomposed by Haar DWT. Then the adaptive thresholding is employed followed by Haar IDWT. The summation of the resulting images constructs the cover image. In the second step, apply Haar DWT on the cover image and the stego image followed by the Alpha blending operation. Then Haar IDWT is performed to get the Arnold scrambled secret image. Finally, perform Arnold transformation with security key to obtain the secret image.

## 3.1 Scrambling based on Arnold Transformation

Arnold transformation, also known as cropping transformation, was proposed by V.J.Arnold while his research of ergodic theory. By representing digital image as a matrix, it becomes "chaotic" after Arnold transformation. The distinct digital image is corresponding to a class of special matrices in which there is a correlation between the elements. After the Arnold transformation of this matrix a new matrix can be obtained in order to achieve image scrambling processing [1]. Setting the image pixel coordinates, N represents the order of the image matrix, i, j ∈ (0, 1, 2, ....., N-1) and the Arnold Transform is as in (1):

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \text{ (Mod N)} \qquad (1)$$

The above transformation is of one-to-one correspondence; the transformation can be done iteratively, iteration number can be used as a private key for extracting the secret image. This transformation gives more security and robustness to the proposed algorithm.

## 3.2 Discrete Wavelet Transform

The wavelet transform is an advanced technique of image analysis. It was developed as an alternative to the Short Time Fourier transform to overcome the problems related to its frequency and time resolution properties [10]. The basic idea of Discrete Wavelet transform (DWT) is to provide the time-frequency representation. The transform is based on wavelets, which are waveforms of limited duration that have an average value of zero. Wavelets are created by translations and dilations of a fixed function called mother wavelet.

The DWT is a mathematical technique for hierarchically decomposing an image or for the multiresolution decomposition of an image [9]. The signal is passed through two complementary filters, which split the signal into high and low frequency parts [2]. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts.

Applying DWT in 2D images, for each level of decomposition, first the DWT is performed in vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, the input image is divided into four non-overlapping multi-resolution sub-bands by the filters, namely LL1, LH1, HL1, and HH1. The sub-band LL1 is referred to as a low-resolution sub-band and high-pass sub-bands LH1, HL1, HH1 as horizontal, vertical, and diagonal sub-band respectively since they represent the horizontal, vertical, and diagonal residual information of the input image [11].

For each successive level of decomposition, the LL sub-band of the previous level is used as the input. To perform the second level decomposition, the DWT is applied to LL1 sub-band which decomposes it further into the four sub-bands namely LL2, LH2, HL2, and HH2. To perform the third level decomposition, the DWT is applied to LL2 sub-band which

decomposes this band further into the four sub-bands namely LL3, LH3, HL3, and HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image, while LL3 contains the lowest frequency band. In case of a 2D image, an N level decomposition can be performed resulting in 3N+1 different frequency sub-bands [8]. The three-level DWT decomposition is as shown in figure 1.

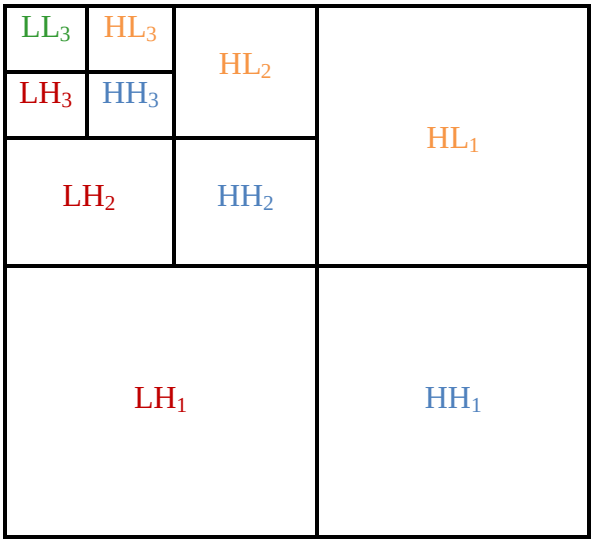


**Fig 1: 3-level DWT decomposition**

## 3.3 Alpha Blending

Alpha Blending is the technique of blending or mixing of two images together to form a final output image. According to the alpha blending formula, the final image is given by (2):

$$FI = I_1 + \alpha * I_2 \quad (2)$$

Where FI - Final Image

$I_1$ - First Image

$I_2$ - Second Image

α can have value between 0 and 1.

## 3.4 Implementation of new proposed steganography method

The proposed method consists of the encoding and decoding processes which are described as follows:

### *3.4.1 Encoding process*

In the encoding process, first the secret image is scrambled (with security key) using the Arnold transformation. Then Haar DWT is applied on the cover image and the Arnold scrambled secret image, which is followed by the alpha blending operation. Then the Haar IDWT is applied to obtain the stego image. This is done using the following algorithm (see figure 2):

Step 1: Obtain the cover image (C) (N*N size) and the secret image (S) (2N*2N size).

Step 2: Apply a 1-level 2-D Haar DWT on the image C (N/2*N/2 size).

Step 3: Apply Arnold transformation with private security key on image S to obtain the Arnold transformed secret image (SS).

Step 4: Apply a 2-level 2-D Haar DWT on the image SS (N/2*N/2 size).

Step 5: Extract the approximation coefficient of matrix LA and detail coefficient matrices LH, LV and LD of 1-level 2-D Haar DWT of the image C.

Step 6: Extract the approximation coefficient of matrix LA1 and detail coefficient matrices LH1, LV1 and LD1 of 1-level 2-D Haar DWT of the image SS.

Step 7: Apply Alpha Blending operation on image C and image SS.

Step 8: Perform 2-D Haar IDWT to obtain the stego image (SI).

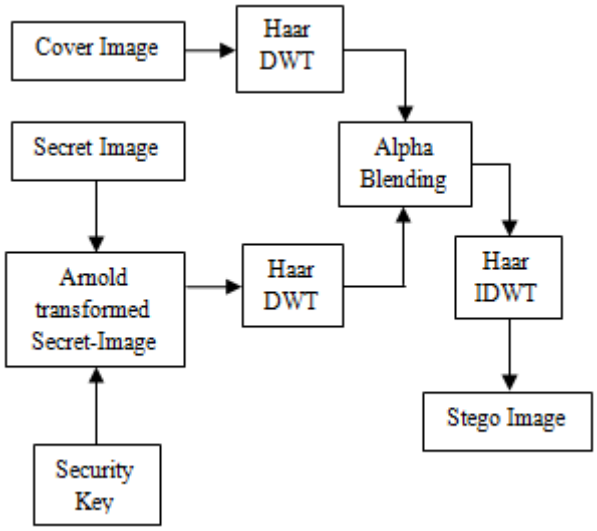


**Fig 2: Encoding Process**

### *3.4.2 Decoding process*

The decoding process is done in two steps:

**A.** In the first step, the cover image is to be recovered from the received stego image. This is done using the following algorithm [12] (see figure 3):

Step 1: Receive the stego image s.

Step 2: Take the logarithmic transform of the received stego image s, to yield another image s'.

Step 3: Using Wiener filter, generate two images $f_1$ and $f_2$. Image $f_1$ is the output of Wiener filter and image $f_2$ is obtained by subtracting image $f_1$ from s'.

Step 4: Apply 2-D Haar DWT on the images $f_1$ and $f_2$.

Step 5: Perform an adaptive denoising method on the coefficients of images $f_1$ and $f_2$ to suppress the noise (secret-image).

Step 6: Apply 2-D Haar IDWT on these denoised images to yield $\hat{f}_1$ and $\hat{f}_2$, the denoised versions of $f_1$ and $f_2$.

Step 7: Add $\hat{f}_1$ and $\hat{f}_2$.

Step 8: Apply the exponential transform to the resulted image so as to obtain the final cover image ĉ (image obtained by denoising the stego image) which is in fact an estimation of c (the original cover image).

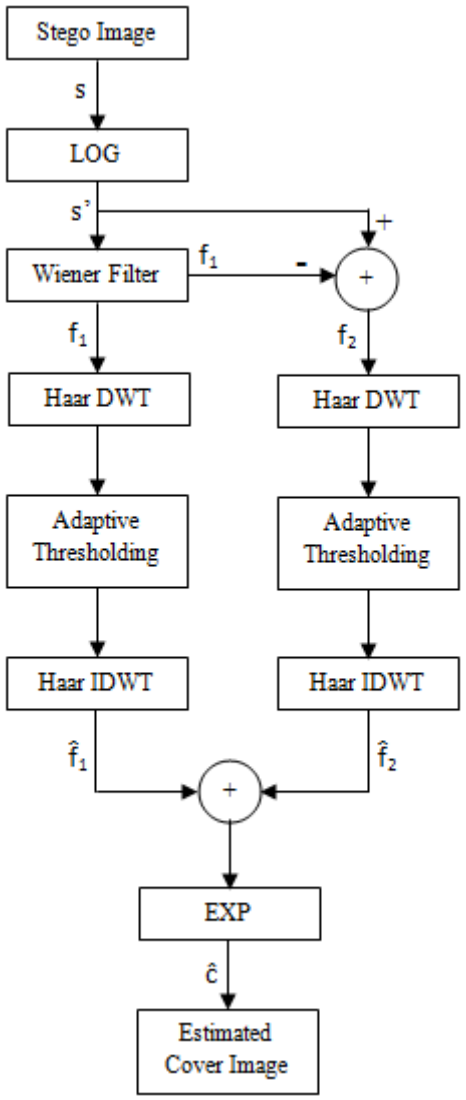


**Fig 3: Process of obtaining the cover image from the stego image.**

**B.** In the second step, the secret image is actually decoded by using the received stego image and the estimated cover image obtained in the above step. First apply 2-D Haar DWT at level 1 on the estimated cover image and the stego image, followed by alpha blending process. Then apply Haar IDWT to obtain the Arnold scrambled secret image. Finally, by applying the Arnold transform with the security key the original secret image is obtained. This is done using the following algorithm (see figure 4):

Step 1: Apply 1-level 2-D Haar DWT on the stego image SI and obtained estimated cover image C.

Step 2: Apply Alpha blending operation on image SI and image C.

Step 3: Separate the wavelet coefficients and apply Haar IDWT to get the Arnold transformed secret image SS.

Step 4: Perform the Arnold transformation with private security key on image SS to get the original secret image S.

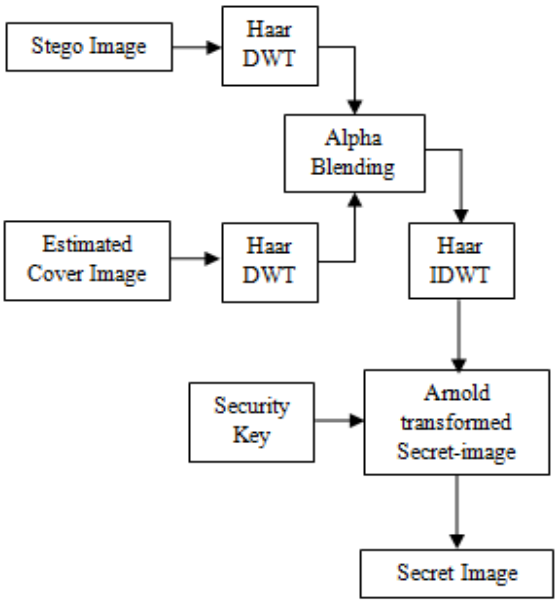


**Fig 4: Process of obtaining the secret image**

## 4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

The performance of the proposed method is evaluated by implementing it using Matlab R2012a and 7.0.1 version. By taking lenna.tiff as the cover image, NAME.bmp as the secret image, the corresponding experimental results are as shown in figure 5.

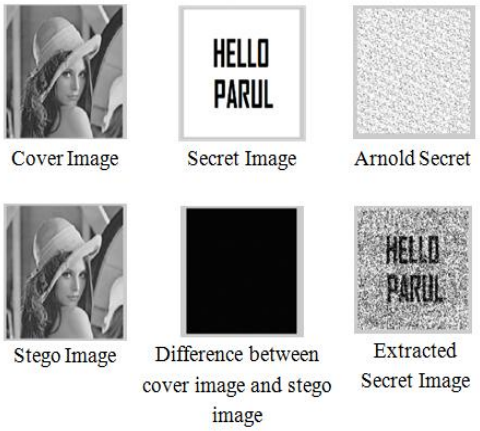


**Fig 5: Shows encoding and decoding process of cover image (lenna.tiff) and secret image (Name.bmp).**

The performance of the proposed method is analyzed by comparing the cover image and the stego image in terms of Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Normalized Cross Correlation (NCC).

PSNR is the measure of the distortion between the original cover image and the stego image [1]. It is defined as follows in (3):

$$\text{PSNR} = 10 \log \frac{255^2}{\text{MSE}} \text{ DB} \quad (3)$$

where MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N [1]. If $x_{j,k}$ and $x'_{j,k}$ are the pixels located at the $j^{th}$ row and $k^{th}$ column of images x and x' respectively, then it is defined as follows in (4):

$$\text{MSE} = \frac{1}{\text{N}} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - x'_{j,k})^2 \quad (4)$$

A large PSNR value indicates the higher image quality (which means there is only little difference between the cover image and the stego image). On the contrary, a small PSNR value indicates that there is great distortion between the cover image and the stego image. It is hard for the human eyes to distinguish between the original cover image and the stego image when the PSNR value is larger than 30db [1]. Also the value of MSE should be as less as possible.

NCC is the measure of the similarity between the original cover image x sized M x N and the stego image x' sized M x N [1]. A positive NCC value indicates the similarity between the cover image and the stego image and the negative NCC value indicates the dissimilarity. It is defined as follows in (5):

$$\text{NCC} = \sum_{j=1}^{M} \sum_{k=1}^{N} x_{j,k} \cdot x'_{j,k} / \sum_{j=1}^{M} \sum_{k=1}^{N} x_{j,k}^2 \quad (5)$$

The proposed method has been tested for the different cover images and secret images for the various values of alpha. Fine tuning the embedding strength factor alpha improves the quality level of stego image and the extracted secret image. The picture quality measurements for some of the tested images have been illustrated in table-1. The results show high PSNR and low MSE values which indicate the effectiveness and accuracy of the proposed method.

## 5. CONCLUSION

A new and secure steganography method for hiding a secret image into a cover image has been proposed. This method does not require the sender to send the cover image along with the stego image to the receiver for the decoding of the secret image. The receiver decodes the secret image by using only the stego image. Experiments show that the proposed method results in good visual quality of the stego image with perceptual invisibility of the secret image and high security.

## 6. REFERENCES

[1] Prabakaran.G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", International Conference on Computing, Electronics and Electrical Technologies, pp. 1096-1100, 2012.

[2] P.Chen, and H.Lin, "A DWT based approach for image steganography", International Journal of applied Science and Engineering", volume 4, 3, pp 275-290, 2006.

[3] H S Manjunatha Reddy and K B Raja, "High Capacity and Security Steganography using Discrete Wavelet Transform", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6), pp. 462-472.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012, pp. 168-187

[5] Narasimmalou, T. and Allen, J.R., "Optimized Discrete Wavelet Transform based Steganography", International Conference on Advanced Communication Control and Computing Technologies, pp. 88-91, 2012.

[6] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal,L. M. Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" International conference on Communication Systems Software, pp. 614-621, 2008.

**Table 1. Comparison of various quality measurements on cover images and stego images with secret images**

| Cover Image | Secret Image | PSNR | MSE | NCC |
|---|---|---|---|---|
| flower.jpg<br>250 X 250 | NAME.bmp<br>403 X 327 | 34.1068 | 1.4454e+006 | 0.9693 |
| flower.jpg<br>250 X 250 | PANGRAM.jpg<br>864 X 540 | 34.1742 | 1.4231e+006 | 0.9698 |
| peppers.tiff<br>256 X 256 | NAME.bmp<br>403 X 327 | 33.7118 | 1.5136e+006 | 0.9696 |
| peppers.tiff<br>256 X 256 | PANGRAM.jpg<br>864 X 540 | 33.7686 | 1.4939e+006 | 0.9699 |
| lenna.tiff<br>256 X 256 | NAME.bmp<br>403 X 327 | 33.9689 | 1.5136e+006 | 0.9688 |
| lenna.tiff<br>256 X 256 | PANGRAM.jpg<br>864 X 540 | 34.0257 | 1.4939e+006 | 0.9691 |
| pirate.tif<br>512 X 512 | NAME.bmp<br>403 X 327 | 34.0077 | 6.0507e+006 | 0.9664 |
| pirate.tif<br>512 X 512 | PANGRAM.jpg<br>864 X 540 | 34.0565 | 5.9831e+006 | 0.9667 |

(PSNR values are measured in DB and other values are in terms of error ratio)

[7] Babita Ahuja and Manpreet Kaur, "High Capacity Filter Based Steganography," International Journal of Recent Trends in Engineering, vol. I, no. I, pp.672-674, May 2009.

[8] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique using DWT and Spread Spectrum", International Journal of Modern Engineering Research, Vol.1, Issue1, pp-157-161.

[9] Nikita Kashyap and G. R. Sinha, "Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)", I.J.Modern Education and Computer Science, 2012, 3, pp. 50-56.

[10] M. Sifuzzaman, M.R. Islam and M.Z. Ali, "Application of Wavelet Transform and its Advantages Compared to Fourier Transform", Journal of Physical Sciences, Vol. 13, 2009, pp. 121-134.

[11] Amitava Nag, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, Volume (4): Issue (6), pp. 561-570.

[12] Arash Vosoughi and Mohammad. B. Shamsollahi, "Speckle Noise Reduction of Ultrasound Images Using M-band Wavelet Transform and Wiener Filter in a Homomorphic Framework", International Conference on Biomedical Engineering and Informatics, pp. 510-515, 2008.

[13] Shikha Sharda and Sumit Budhiraja, "Image Steganography: A Review", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 1, January 2013, pp. 707-710.