International Journal of Computer Science and Business Informatics

IJCSBI.ORG

Implementation of Image Steganography Using 2-Level DWT Technique

Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal

Department of Computer Science and Engineering,
Inderprastha Engineering College,
Gautam Buddh Technical University

ABSTRACT

Image steganography is an engineering term defining a different and significant discipline for information hiding. This process can be described as 'hiding of secret information behind an image'. Discrete Wavelet Transform (DWT) is one of the known methods used in steganography. The focus of the proposed work in this paper is on decreasing the complexity in image hiding through DWT technique while providing better undetectability and lesser distortion in the stego image. This paper proposes the algorithm for embedding and extracting the secret image embedded behind the cover gray scale image. Also, the analysis of performance measurement methods such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), gives us the experimental summary for four different cases where each case spans different sizes of cover and secret image, comparing the cover image and stego image at the sender's side and embedded secret and extracted secret at the receiver's side. The stego attacks are then applied on the stego image and after each of the attack, the secret image is extracted from the distorted image. For better analysis, this extracted secret is compared with the expected result on the basis of PSNR and MSE. Also, the proposed algorithm is compared with one of the existing method using DWT technique, proposed by K.B. Shiva Kumar et. al. [7].

Keywords
Cover image, DWT, Key information, Secret image, Stego image

1. INTRODUCTION

Image steganography has been a vast area of research for many years now. It is a process that hides the secret image behind the cover image in such a way that the presence of the secret image is locked and the cover image appears to be the same [1]. In such a way, the digital information can be embedded and transferred to the destination with minimum risk of detectability. The concept of 'undetectability' has raised the need of steganography in all dimensions such as commerce, national security services, and banking and other private communication areas. Other information hiding methods such as cryptography, watermarking and digital signature differs from the steganography concept as steganography allows

the communication to be hidden and also, provides better quality of the secret image.

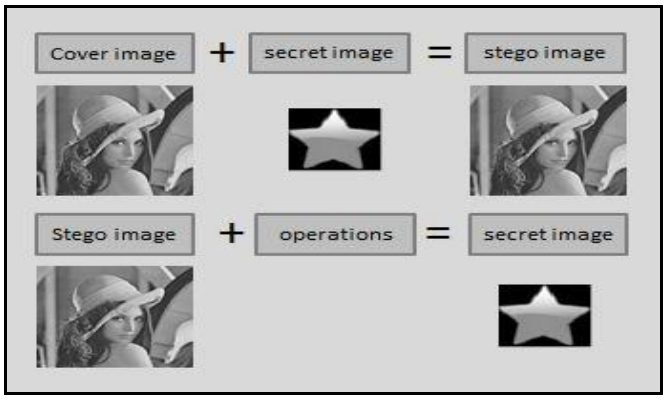

Figure 1. Principles of Steganography

Figure 1 shows the basic flow of processes that takes place in image steganography. The steganography [2] is a two sided method where on the one side the secret image is embedded in the cover image and on the other side, the secret image is extracted by performing inverse operations on the stego image.

In this paper, the discrete wavelet transform (DWT) technique is used to accomplish the embedding of the image which is one of the most robust, secure and high capacity image steganographic techniques.

2. DISCRETE WAVELET TRANSFORM (DWT)

Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis [3]. The DWT approach applied in the proposed work is the 'Haar DWT', simplest of all the wavelet transform approaches. In this transform, time domain is passed through low-pass and high pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively [4]. The operation of Haar DWT on the cover image results in the formation of 4 sub-bands, namely the approximate band (LL), horizontal band (HL), vertical band (LH) and the diagonal band (HH). The approximate band contains the most significant information of the spatial domain image and other bands contain the high frequency information such as edge details. Thus, the DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution. This process can be

iterated on one of the sub-band of first level DWT to get the further second level sub bands for better results.

LL	HL
LH	HH

Figure 2. Sub bands formed after applying Haar DWT [4]

Figure 2 shows the 4 sub-bands that are formed after applying 1-level Haar DWT on a 2-dimensional image.

3. STEGANALYSIS

Steganalysis [5] is an art of identifying stego images that contains a secret image. However it does not consider the successful extraction of the secret image, which is a requirement for cryptanalysis. Steganalysis is a very difficult task as it is based on insecure steganography. Recently, steganalysis has received a lot of attention from the media and the legal world. The attacker either can destroy, disable the secret image or may also add counter information over the original secret image which leads to statistical differences of the secret image.

4. PROPOSED MODEL

The model proposed in this paper is a unique attempt to simplify the embedding procedure and reduce the effort of concealing the secret image in the cover image and yet offering better results. The model can be broadly divided into two sub modules where one module deals with the proper concealing of secret image and the other module extract the secret image. The models are explained in a step-wise procedure below.

4.1 Embedding model

This model will take the cover image and secret image as inputs and will output the stego image which appears to be the same as the cover image but will have the secret image within it.

STEP 1 - Input the cover image and then apply the 2-level DWT transform on the image. This will result in the formation of four bands i.e. LL1, HL1, LH1 and HH1. Now for better imperceptibility, the DWT transform is applied once again on the HH band to get the next coarser scale of wavelet coefficients resulting in another level of sub-bands in HH1 band as LL2, HL2, LH2 and HH2. Here, the LL2 band is selected to embed the secret

because hiding in the approximate band will result in a smooth and better extraction of the secret at the receiver's side.

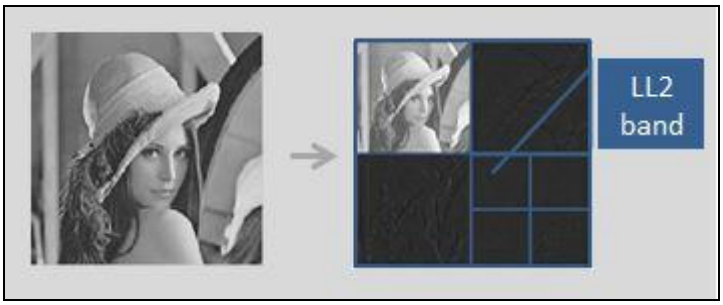

Figure 3. 2-level DWT operation on cover image

STEP 2 - Starting from the top left corner of the LL2 level band, replace the 5 LSB of the LL2 band coefficient by 5 MSB of the secret image pixel.

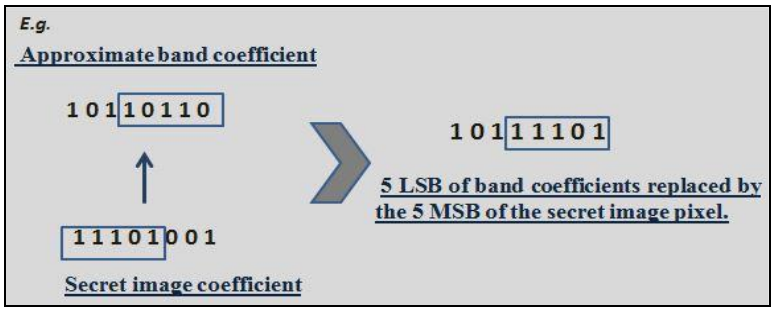

Figure 4. Example depicting the operation

STEP 3 - Iterate the above step for n times (where n*n is the size of the secret image) and hence we get the embedded secret.

Figure 5. Secret image embedded

Figure 6. Stego image

STEP 4 - Apply inverse DWT twice to retranslate the frequency domain information to the spatial domain and hence we obtain the stego image which appears to be the same as the cover image.

The stego image so formed is transferred over the public network with the least risk. The key information is also sent to the receiver, because without the prior knowledge of key info the secret image cannot be extracted. The key info is the random combination of the size of the secret image, the name of the band where the secret is embedded and the number of MSB bits of the secret embedded.

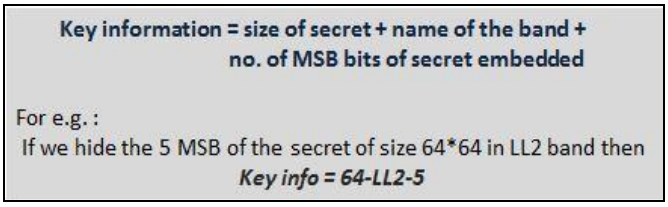

Figure 7. Key information

Figure 7 shows the detailed concept for the generation key information by the sender, which is sent to the receiver along with the stego image.

4.2 Extracting model

The stego image is taken as input in this model and the secret image is extracted out of it, after processing it according to the key information. The extraction model is simpler than the embedding module, as it is just the reverse process of embedding. It simply employs the Haar DWT operations and the corresponding extraction of the MSB of the secret.

STEP 1 - The stego image is loaded as the input. The receiver has the prior knowledge of the location of the secret as it is provided in the form of key information. Thus to obtain the required band, the stego image is transformed to the frequency domain from the spatial domain by applying the 2 level DWT operations over it. After this step, the receiver has the LL2 band wherein it contains the secret image's bits.

Figure 8. 2-level DWT operation on received image

STEP 2 - Starting from the top left corner of the 2nd level approximate band i.e. LL2 band, extract the 5 LSB into a new matrix vector.

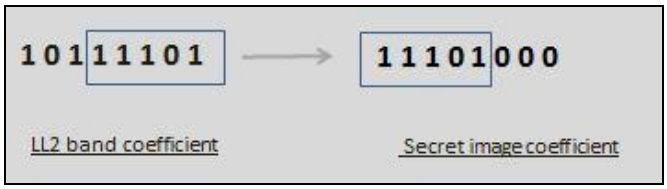

Figure 9. Example depicting the operations

STEP 3 - After iterating the above step n times (where n is the size of the secret image as provided by the sender, included in the key information X), we get the secret image in an n*n matrix.

Figure 10. Secret image extracted

5. THE BASIC ALGORITHM

The basic steps involved in the entire process as explained in the proposed model can be enumerated in an algorithmic way showing the proper flow of operations.

5.1 *Embedding Algorithm*

1. Input the cover image.
2. Apply the 2-level DWT on the cover image.
*3. Select the band to be modified as '**m**' (i.e. LL2).*
4. Input the secret image.
*5. Obtain the size of the secret as '**n**'.*
*6. For each of the n*n coefficient of the m band replace the '**p LSB** bits' (i.e. 5 bits) by the '**p MSB** bits' of the secret image.*
7. Apply IDWT (Inverse DWT) operation twice and the stego image is obtained.
*8. The key information is formed as: **K** = n + m + p.*

5.2 *Extracting Algorithm*

1. Input the stego image.
2. Apply 2-level DWT transform on the stego image.
3. Load the key information K and assign the corresponding values in m, n and p.
4. Starting from the top left corner of the m band, extract the 'p LSB' of the

band coefficient to the 'p MSB' of the new matrix vector.
5. Repeat this step for n times in both dimensions and name this new matrix vector as the secret image.
6. Output the secret image.

6. STEGO ATTACKS

The stego image so formed at the end of the embedding module, when passed over the public network, then an intruder may acquire the stego image and can willingly modify this image to distort the secret hidden behind it. The algorithm which we propose in this paper is robust to various kinds of stego attacks.

6.1 Geometric Attacks

These attacks are applied on the 2D matrices formed of the stego image such as rotation, scaling and translation. Figure 11 shows the distortion created in the stego image and corresponding extracted secret images.

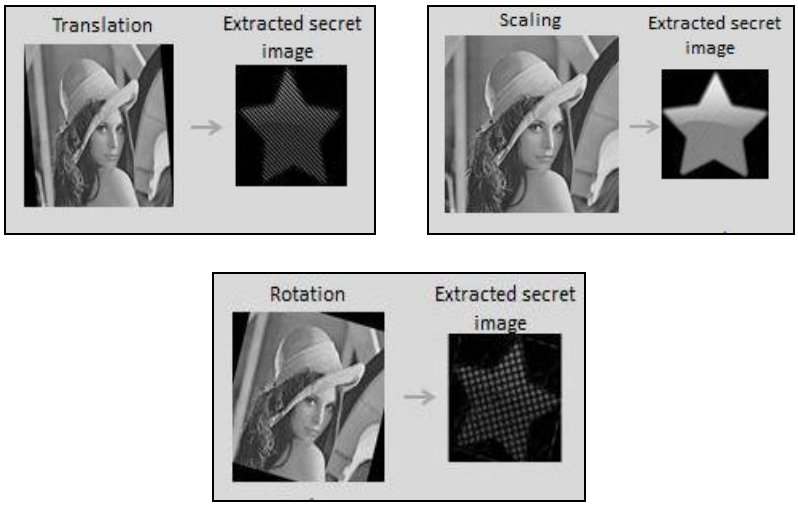

Figure 11. Extracted secret images after applying Geometrical distortions

Figure 11 shows the extracted secret image which is translated, scaled and rotated corresponding to the translation, scaling and rotation of stego image. When the stego image is rotated, then the secret image, which is stored in LL2 band's coefficients in a right to left and top to bottom sequential manner also gets rotated and hence we get the rotated extracted secret. The same happens with other geometrical attacks too, as shown above.

6.2 Adding Noise

These attacks are applied on the stego image by adding noise such as Gaussian noise, salt and pepper noise and speckle noise.

The figure below shows the application of these noises, with default amount of noise on the stego image and the extracted secret images for each case.

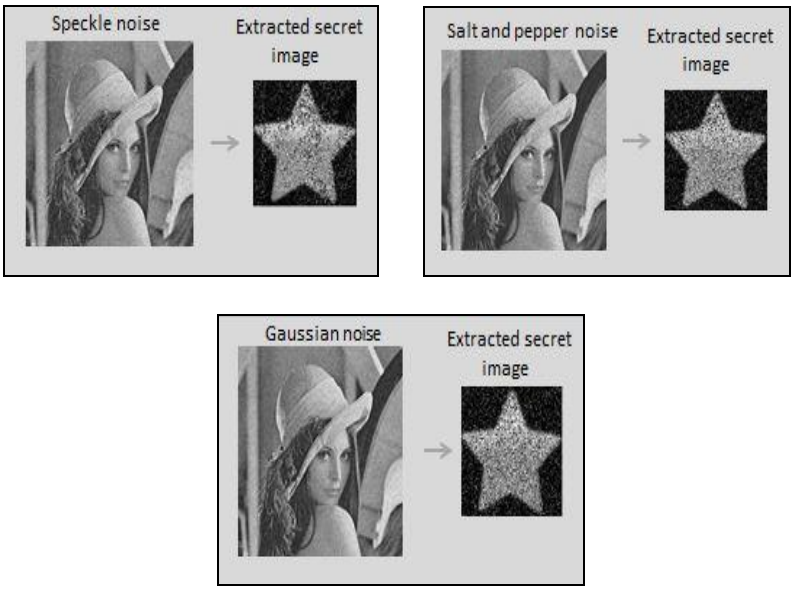

Figure 12. Extracted secret images after applying noise

Figure 12 shows the extracted secret image which is added with speckle, salt and pepper and Gaussian noise corresponding to the noised stego image.

6.3 Pixel Arithmetic

These attacks are directly applied on the pixels of the stego image such as transpose, thresholding, brightening and darkening. The figure given below explains the application of these kinds of attacks and the corresponding extracted secrets.

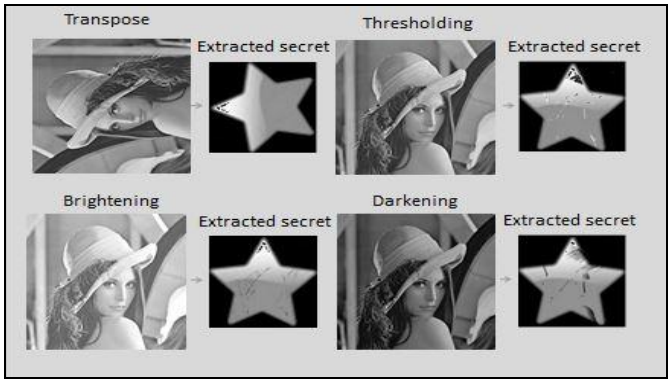

Figure 13. Extracted secret image after pixel arithmetic operations

Figure 13 shows the extracted secret image which is transposed, threshold, brightened and darkened corresponding to the transposed, threshold, brightened and darkened stego image.

7. QUALITY MEASUREMENT TECHNIQUES

The quality of the stego image and the extracted secret image is measured by calculation of certain quality measurement metrics [6]. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values. The metrics used in this paper are as follows:

7.1 Peak signal to noise ratio (PSNR)

The PSNR depicts the measure of reconstruction of the compressed image. This metric is used for discriminating between the cover and stego image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR = 10 \log 255^2 / MSE \quad \text{...Eq.1 [6]}$$

A low value of PSNR shows that the constructed image is of poor quality.

7.2 Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [6] can be defined as the measure of average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - f'(i,j))^2 \quad \text{...Eq.2 [6]}$$

Where f (i, j) is the original image and f' (i, j) is the stego image. A large value for MSE means that the image is of poor quality.

7.3 Normalised Correlation (NK)

Normalised Correlation measures the similarity between the two images, i.e. the original image and the stego image. Larger values of NK indicate poorer image quality. Its value tends to one as the difference between the two images tends to zero [6]. Normalised Correlation is formulated as:

$$(NK) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j).f'(i,j)]}{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)^2} \quad \text{...Eq.3 [6]}$$

7.4 Normalised absolute error (NAE)

The NAE [7] is the measure of how distant is the modified image from the original image with the value of zero being the perfect fit. The normalised absolute difference can be calculated as:

$$NAE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|\ [f(i,j).f'(i,j)]\ |}{\sum_{i=1}^{M}\sum_{j=1}^{N}|\ f(i,j)\ |} \quad \text{...Eq.4 [6]}$$

8. EXPERIMENTAL SUMMARY

On the basis of the formulae discussed above, various set of cover and secret images are compared. The cover images and the secret image used are shown below in Figure 14 and Figure 15, respectively.

Figure 14. Cover images (.bmp)

Figure 15. Secret Image embedded (.bmp)

CASE 1	***CASE 3***
Size of Cover = 256*256	Size of Cover = 512*512
Size of Secret = 32*32	Size of Secret = 64*64
CASE 2	***CASE 4***
Size of Cover = 256*256	Size of Cover = 512*512
Size of Secret = 64*64	Size of Secret = 128*128

Figure 16. Four cases for various set of sizes of cover and secret image.

Figure 16 shows the four cases with, each with varied set of sizes of cover and secret image.

8.1 Comparison between cover image and stego image

The table given below shows the value of the PSNR and MSE presenting the comparison between the original cover image and the stego image formed at the end of the embedding module for all the four cases defined.

Table 1. PSNR and MSE values

COVER IMAGE V/S STEGO IMAGE								
Cover	CASE 1		CASE 2		CASE 3		CASE 4	
Image	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
lena	54.15	0.25	47.60	1.12	55.95	0.16	51.37	0.47
boy	56.17	0.14	50.03	0.64	56.24	0.15	52.07	0.40
spider	54.92	0.19	49.09	0.79	56.03	0.13	51.79	0.43
jet	54.65	0.22	48.26	0.97	55.31	0.19	51.02	0.51
rose	55.65	0.17	49.38	0.75	56.03	0.16	51.88	0.42

The highlighted region in Table 1 shows that the maximum PSNR value obtained, is 56.24 dB for case 3 (cover size- 512*512 and secret size- 64*64), which is a very high value.

8.2 Comparison between embedded secret image and extracted secret image

The table given below shows the value of the PSNR and MSE presenting the comparison between the embedded secret and the extracted secret formed obtained at the end of the extracting module for all the four cases.

Table 2. PSNR and MSE values

EMBEDDED SECRET IMAGE V/S EXTRACTED SECRET IMAGE								
Cover	CASE 1		CASE 2		CASE 3		CASE 4	
Image	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
lena	18.03	1.025	17.98	1.036	17.97	1.041	17.98	1.037
boy	17.99	1.019	17.92	1.048	17.94	1.042	17.95	1.044
spider	18.01	1.027	17.97	1.037	17.96	1.040	17.98	1.036
jet	18.02	1.028	17.99	1.038	17.98	1.039	17.99	1.035
rose	18.01	1.03	17.96	1.040	17.95	1.041	17.96	1.041

Table 2 shows the PSNR and the MSE values for each case. The PSNR values ranges from 17 dB to 18 dB, which is a fair enough value when the smaller sized images are compared.

8.3 Comparison between embedded secret and extracted secret after applying stego attacks

The table given below shows a PSNR comparison for one of the case (i.e. *case 4, where size of cover and secret is 512*512 and 128*128* respectively) between the secret image embedded at the time of embedding and the extracted secret after applying various stego attacks.

Table 3. PSNR value for case 4 after applying attacks

STEGO ATTACKS	PSNR
Geometrical Distortions	
Rotation	7.471
Scaling	9.037
Translating	8.142
Adding Noises	
Gaussian noise	11.575
Salt & Pepper noise	11.325
Speckle noise	11.517
Pixel Arithmetic	
Transpose	10.314
Thresholding	12.895
Brightening	12.737
Darkening	13.063

Table 3 shows the PSNR value, comparing the embedded secret and extracted secret after distortion of stego image (for case 4 only)**,** which ranges from 7 to 13 dB which is approximately 40%-75% of the PSNR value obtained (from Table 2) while comparing the embedded secret and extracted secret when no attack was performed on the stego image.

9. SIMULATION RESULTS

In this section, an experiment is carried out to prove the efficiency of the proposed method. The proposed scheme has been simulated using MATLAB 7.6 running on a Windows 7 platform. An 8-bit grayscale image of 256*256 is used as the cover image to form the stego image, concealing a 90*90 secret image. Both, the secret image and the cover image are in the '.png' format.

Figure 17. Boatman.png

Figure 18. Pout.png

Our proposed algorithm was applied on this set of cover image and secret image with the given size, and the respective PSNR is calculated. Then the PSNR generated by one of the existing method, proposed by in [7] was compared with our PSNR values.

Table 4. Comparison of Results

PSNR VALUE	
EXISTING METHOD	PROPOSED METHOD
32.18	**46.77**

The PSNR value for the original cover image and the stego image, as computed by our proposed method was found better than the existing method [7], as the PSNR value comparing cover image and stego image, calculated from our proposed method is 45% more than the PSNR value calculated from one of the existing method [7].

10. CONCLUSIONS

The proposed model for image steganography is a simple, secure, robust technique for image hiding providing good embedding capacity of secret, where the maximum size of secret allowed is ¼th of the size of the cover image. The stego image formed using this proposed algorithm appears to be the same as the cover image offering the high PSNR value as shown in Table 1 and Table 2. The stego image is partially robust to various geometrical and statistical attacks but ensures to deliver the exact pattern of the secret to the receiver even if the stego image appears to be highly distorted. The PSNR value, comparing the embedded secret and extracted secret after distortion of stego image is approximately 40%-75% of the PSNR value comparing the embedded secret and extracted secret when no attack was performed on the stego image. Also the PSNR value of the original cover image and the stego image, as computed by our proposed method was found 45% more than the PSNR value calculated from the existing method.

11. REFERENCES

[1] L. Marvel, C. G. Boncelet, Jr, and C. T. Retter, "Spread spectrum image steganography*", IEEE Trans. Image Process.*, Vol. 8, No. 8, pp. 1075–1083, Aug. 1999.

[2] Ying Wang, Pierre Moulin, "Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions," *IEEE Trans. On Information Theory*, Vol. 54, No. 6, June 2008.

[3] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering* 2006. Vol 4, No. 3, pp 275-290.

[4] Yedla Dinesh and Addanki Purna Ramesh, "Efficient Capacity Image Steganography by Using Wavelets ", *International Journal of Engineering Research and Applications* (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp 251-259.

[5] Miss. Prajakta Deshmane, Prof. S.R. Jagtap,"Skin Tone Steganography for Real Time Images", *International Journal of Engineering Research and Applications* (IJERA), Vol. 3, Issue 2, Mar-Apr 2013, pp 1246-1249.

[6] Sumathi Poobal, G. Ravindran,"The Performance of Fractal Image Compression on Different Imaging Modalities Using Objective Quality Measures," *International Journal of Engineering Science and Technology (IJEST),* Vol. 2, Issue 1, Jan-Feb 2011, pp 239-246

[7] K B Shiva Kumar ,K B Raja ,R K Chhotaray, Sabyasachi Pattnaik ,"Performance Comparison Of Robust Steganography Based On Multiple Transformation Techniques," *International Journal of Comp. Tech. App.*, Vol. 2(4), July-Aug 2011, 1035-1047.