A LWT and DCT based Blind Watermarking Scheme for Digital Images

Amy Tun, Dr.Yadana Thein
University of Computer Studies, Yangon
amytun05@gmail.com

Abstract

As a potential solution to defend unauthorized replication of digital multimedia objects, digital watermarking technology is now attracting significant attention. With a combination of Lifting Wavelet Transform (LWT) and Discrete Cosine Transform (DCT), the system is presented. Key sequences used for watermark embedding and extraction are generated by Linear Congruential Generator (LCG). Moreover, for the sake of security enhancement, double coded image puzzling method is created. The LWT is applied to decompose the original image into four sub-band images. Then the DCT is computed on the selected sub-band of the LWT coefficients. The watermark bits are modified by LCG and embedded in the DCT transformed of the selected LWT sub-band of the original image. The Double-coded image puzzling is created in order not to recognize the meaningful image by illegal users. The proposed system mainly focuses on an invisible watermark embedding, imperceptibility of watermarked image, blind watermarking by using key sequence instead of using original image, and robustness for watermark extraction. The presented system is realized in MATLAB.

1. Introduction

Digital watermarking technology for multimedia contents as the field of information hiding technology is a useful way in dealing with the copyright protection problem. Digital image watermarking is the process of embedding additional information into an image to make assertion about the image. The embedded information is called watermark which is, in general, a visible or invisible identification code that may contain owner’s information. The presented system mainly consists of the watermark structure, an embedding process, an extraction process, random number sequence generation for blind extraction, and double-coded image puzzling for security enhancement.

Digital image watermarking schemes can be placed under two categories based on whether or not they use the original image for extraction of watermark from watermarked image such as blind watermarking techniques which do not require original image and non-blind watermarking that requires original image to exist for detection.

Moreover, there are two main directions for embedding, namely the spatial and the frequency domain. Watermark information is directly embedded into image pixels by the spatial domain methods. The frequency domain approaches are the most successful and popular for image watermarking. Two major applications of digital watermarking are copyright protection and data authentication. The quality of watermarked image is measured by Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Human Visual System (HVS).

In the paper, Digital image watermarking algorithm is described based on combining two transforms; LWT and DCT. Watermarking is done by altering the wavelets coefficients of carefully selected LWT sub-bands (HH), followed by the application of the DCT transform on the selected sub-bands. The watermark is coded by using LCG and double coded system. The rest of the paper is organized as follows: A brief review of some of the works available in the literature that utilizes watermarking for copyright protection in frequency domain is given in Section 2. The proposed blind watermarking approach is presented in section 3. Finally, the conclusions are summed up in section 4.

2. Related Work

A number of earlier works related to digital image watermarking inspired us to do this research. Some of such recent researches are briefly described in this section.

M. Jiansheng, L. Sukang and T. Xiaomei [5] have proposed an algorithm of digital watermarking based on DCT and DWT. The system showed that the algorithm has strong capability of embedding signal and anti-attack.

Dr. Ekta Walia and Payal Jain [10] presented that analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography. LSB based Steganography embed the text message in least significant bits of digital picture.DCT based Steganography embed the text message in least significant bits of the Discrete Cosine (DC) coefficient of digital picture. In which, DCT based steganography scheme is recommended because of the minimum distortion of image quality.

Yang Jie described that Traditional Arnold transform used in information hiding technology introduces an new anti-Arnold transform algorithm, which reduces iterative times of anti-transform. With the combination of image blending, discrete cosine transform and new anti-Arnold transform, an algorithm based on the three technologies is proposed. [6] In which, experimental result are shown that the algorithm has good imperceptibility and validity.

S. S.GONGE and et al. [3] discussed Security of Still Image by Using Digital Watermarking Technique by Using Discrete Cosine Transform and Spread Spectrum. It is shown that the technique provides the security for the digital image which is used for copyright protection. K. Hameed and et al. reviewed the various watermarking techniques in the wavelet transform domain [4] and simulated two of the techniques in detail to analyze the robustness for copyright. It can be seen that both the techniques were found non-obtrusive in gray level images.

3. Watermarking Approach in Frequency Domain

This section details the proposed blind watermarking scheme for copyright protection of digital images. The following subsections present the steps involved in the watermark embedding and extraction processes along with a brief description about the lifting wavelet transform (LWT), discrete cosine transform (DCT), Linear Congruential Generator (LCG) and Double coded image Puzzling.

3.1. Lifting Wavelet Transform (LWT)

Lifting Wavelet Transform as shown in Figure.1 based on the traditional wavelet is introduced by Wim Sweldens, using a simple relationship among all multi-resolution analyses with the same scaling function. The lifting scheme has several virtues compared with the traditional wavelet such as LWT can compute more effectively and needs smaller memory space and the transform coefficients from LWT are integers, overcoming the weakness of quantizing errors from the traditional wavelet transform. As the basic idea of integer wavelet transform, lifting wavelet transform consists of the following steps: split, predict and update [8].

(1) **Split**: The original data set x[n] is divided into two disjoint subsets including odd subset $\mathbf{x_o[n] = x\ [2n+1]}$ and even subset $\mathbf{x_e\ [n] = x\ [2n]}$.

(2) **Predict**: The error in predicting x_o[n] from x_e [n] using prediction operator P is generated as the wavelet coefficients d [n] as in (1).

$$\mathbf{d\ [n] = x_o[n] - P\ (\ x_e\ [n])} \qquad (1)$$

(3) **Update**: Scaling coefficients c[n] that represent a coarse approximation to the original signal x_e[n] are obtained by combining x_e[n] and d[n]. This is accomplished by applying an update operator U to the wavelet coefficients and adding the result to x_e [n] as in (2).

$$\mathbf{c\ [n] = x_e\ [n] + U\ (d[n])} \qquad (2)$$

Transformation of the whole image introduces inherent scaling. It shows better identification of which data is relevant to human perception higher compression ratio. Wavelet function can be freely chosen. The main virtue of the LWT is perfect reconstruction of the image using approximation coefficients and detail coefficients, obtained by lifting wavelet decomposition.

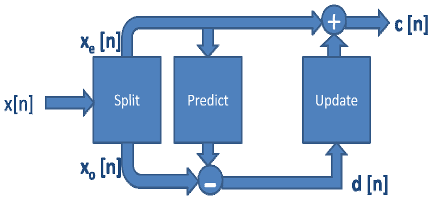


Figure 1. Lifting Wavelet Transform

3.2. Discrete Cosine Transform (DCT)

A technique for converting a signal into elementary frequency components is the discrete cosine transform. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image, x, the DCT coefficients for the transformed output image, y, are computed according to (3) shown below. In the equation, x is the input image having M x N pixels, x (m, n) is the intensity of the pixel in row m and column n of the image, and y (u, v) is the DCT coefficient in row u and column v of the DCT matrix [9].

(3)

Where

= if u=0 or = 1 if u=1,2,…,N-1.

= if u=0 or if v=1,2,…,N-1.

The popular block-based DCT transform segments an image on non-overlapping blocks and applies DCT to each block. These results in giving three frequency sub-bands: low frequency sub-band, mid-frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression [1,7,2,11].

3.3. Linear Congruential Generators (LCG)

The simple form of the linear congruential generator is $x_i = (ax_{i-1}+c) \bmod m$, with . The modular function has four parameters: a is the multiplier, x_0 is the seed-value from which consequent x_i values are calculated, c is the increment value, and m is the modulus of the generator. It’s not uncommon to see a linear congruential generator with c=0, in which case the generator is called a multiplicative congruential generator. The LCG is a practical and efficient generator whose output is sufficiently random.

3.4. Double-coded Image Puzzling

The image puzzling is reallocation of the blocks of the original image, which is firstly separated into blocks by blocks. The main idea is to degrade the original image so that it cannot be shown at once seen. On the other hand, the idea is to enhance the security of the image. The puzzled image is used to create code by combining with LCG to embed image to get security features. It is not easy to recognize.

3.5. Watermark Embedding Process

The watermark embedding procedure design as shown in Figure 2 is followed by a detailed explanation.

Step 1: Read in the original image f(x, y) as shown in Figure 3.

Step 2: Apply LWT to decompose the cover image f into four non-overlapping multi-resolution sub-bands: LL, HL, LH, and HH as shown in Figure 4. From the four sub-bands, choose HH sub-band for embedding the watermark image.

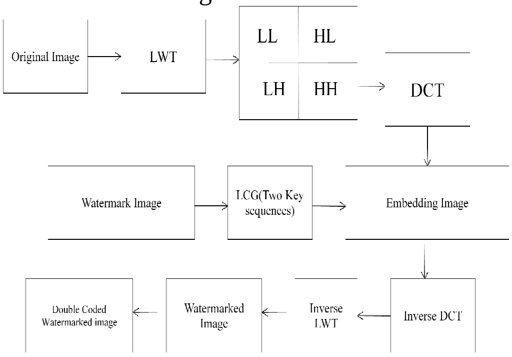
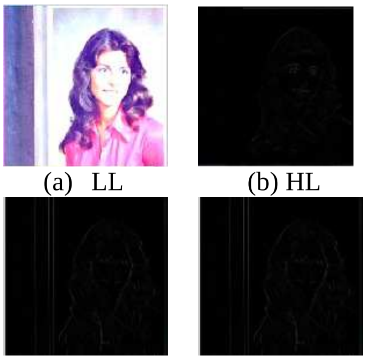


Figure 2. Watermark Embedding Procedure using LWT-DCT Double Coded Image Puzzling method

Figure 3. Original image



(a) LL (b) HL

(c) LH (d) HH

Figure 4. Lifting Wavelet Transform

Step 3: Divide the sub band HH into 8x8 blocks.

Step 4: Apply DCT to each 8x8 block in the chosen sub-band (HH).

Step 5: Read in the binary watermark image as shown in Figure 5.

Figure 5. Watermark

Step 6: Generate two uncorrelated LCG sequences which are used to embed the watermark bit 0 (PN0) and watermark bit 1 (PN1).

Step 7: Embed the two pseudorandom sequences, PN0 and PN1, with a gain factor, in the DCT transformed of the selected LWT sub-bands of the host image. If X is denoted as the matrix of the mid-band coefficients of the DCT transformed block, then embedding is done according to Equation (4) and (5).

If the watermark bit is 0 then

$$\mathbf{X' = X + k * PN0} \qquad (4)$$

Otherwise,

If the watermark bit is 1 then,

$$\mathbf{X' = X + k * PN1} \qquad (5).$$

Where X ' is watermarked DCT block.

Step 8: Apply inverse DCT (IDCT) to each block after its mid-band coefficients have been modified to embed the watermark bits as described in the previous step.

Step 9: Apply the inverse LWT (ILWT) on the LWT transformed image, including the modified sub-band, to produce the watermarked host image as shown in Figure 6.

Figure 6. Watermarked Image

Step 10: Double code sequence is created by combining LCG and image puzzling code. The original image cannot be easy to recognize by applying such codes as shown in Figure 7.

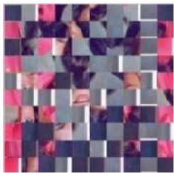


Figure 7. Double Code Puzzled Image

The idea of using the double-coded sequences is so that the watermarked image cannot be recognized at once when an attacker discovers the image. The sequence generated first phase by using LCG is required each time when both embedding and detecting watermark for blind watermarking. Using a double code to encode a watermark, the owner's data can be secure and will not be perceived by any intermediary party. The original watermark can only be decoded by using the same secret sequence. The double coding Algorithm is as follows:

Double Coding Algorithm

- Input: A Watermarked Image, rows, cols, actual_row, actual_col
- Output: code of the watermarked image

```
Begin
    startrow1=1; endrow1= actual_row;
    startcol1 =1; endcol1=actual_col;
    startrow2 = actual_row + 1;
    endrow2= actual_row + actual_row;
    startcol2=actual_col+1; endcol2=actual_col+
    actual_col;
    startrow3=endrow2 + 1;
    endrow3= rows;
    startcol3=endcol2 +1; endcol3=cols;
block1=Image(startrow1:endrow1,startcol1:endcol1);
block2=Image(startrow2:endrow2,startcol1:endcol1);
block3=Image(startrow3:endrow3,startcol1:endcol1);
block4=Image(startrow1:endrow1,startcol2:endcol2);
block5=Image(startrow2:endrow2,startcol2:endcol2);
block6=Image(startrow3:endrow3,startcol2:endcol2);
block7=Image(startrow1:endrow1,startcol3:endcol3);
block8=Image(startrow2:endrow2,startcol3:endcol3);
block9=Image(startrow3:endrow3,startcol3:endcol3);
    code=Code_fun(block1,block2,block3,block4,blo
    ck5,block6,block7,block8,block9);
End
```

In the embedding process, the watermarked image is obtained with no loss of the image quality after step 9 is completely finished. Step 10 is the enhancement stage for image security.

3.6. Watermark Extraction Process

The watermark embedding procedure design as shown in Figure 8 is followed by a detailed explanation.

Step 1: Apply LWT to decompose the watermarked double-coded image as shown in Figure 7 into four non-overlapping multi-resolution sub-bands: LL, HL, LH, and HH.

Step 2: Divide the sub-band HH into 8x8 blocks.

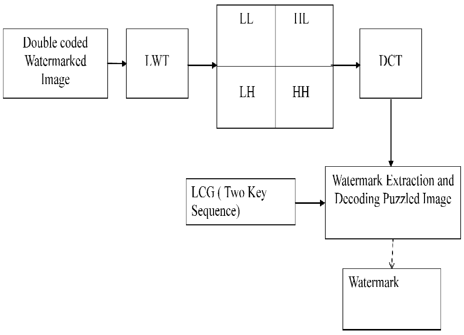

Double coded Watermarked Image
LWT
LL
HL
LH
HH
DCT
LCG (Two Key Sequence)
Watermark Extraction and Decoding Puzzled Image
Watermark

Figure 8. Watermark Extraction Procedure using LWT-DCT Double Coded Image Puzzling method

Step 3: Apply DCT to each block in the chosen sub-band HH, and extract the mid-band coefficients of each DCT transformed block.

Step 4: Regenerate the two pseudorandom sequences PN0 and PN1 using the same seed used in the watermark embedding procedure.

Step 5: For each block in the sub band HH, calculate the correlation between the mid-band coefficients and two generated pseudorandom sequences (PN0 and PN1). If the correlation with the PN0 is higher than the correlation with PN1, then the extracted watermark bit is considered 0, otherwise the extracted watermark is considered 1.

Step 6: Reconstruct the watermark using the extracted watermark bits and compute the PSNR between the original and extracted watermark.

3.7. Performance Evaluations

The performance of the proposed scheme is evaluated in terms of the quality of the watermarked image with various pixels by pixels sizes, and the robustness of the watermark against attacks with good resistance level. The peak signal to noise ratio (PSNR) is typically used as a measure of the quality of a watermarked image. PSNR in decibels (dB) is given by,

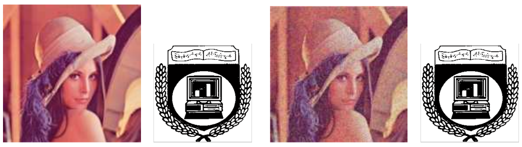
(6)

The original image is f(x, y) and the watermarked image is F(x, y). N is the number of pixels. MSE means Mean Square Error.

Invisible watermark embedding can be evaluated with Human Visual System (HVS). Several images bearing different visual and spectral characteristics are used. The standard images (Lena, peppers) were primarily used along with some others. Moreover, non-standard images are also used.

3.7. 1 Tests and Results of Robustness to Noise Attack

To archive the high reliability of watermark, the watermark extraction process has to be robust to the alterations in the watermarked image caused from both unintentional and intentional distortions. The presented system describes that it can handle the robustness issues against noise addition to image watermarking scheme by extraction the watermark. It is clearly shown in Figure 9 that the watermark can be extracted from noise attacked watermarked image. In which, the original image is standard images such as Lena with 512x512 pixels as shown in Figure 9.(a). The watermark use UCSY logo with sizes of 256x256 pixels as shown in Figure 9.(b). In the testing, the watermarked image is added salt and pepper noise with the amount of 20% of the whole image as shown in Figure 9.(c). The watermark can still be extracted from watermarked image as shown in Figure9.(d). The PSNR value for before noise attacking is 41.7263dB and the value after attacking is 30.1683 dB.

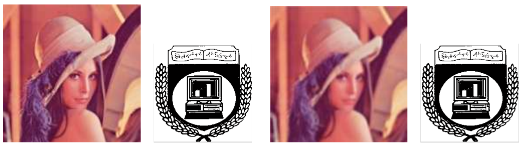


(a) (b) (c) (d)

Figure 9. Robustness to Noise Attack

3.7.2 Tests and Results of Robustness to Filtering Attack

This watermarking scheme has been tested against several attacks including Gaussion low-pass filtering. The system describes that it can prove the robustness issues of image watermaking scheme by extraction the watermark from filtering attacked watermarked image as shown in Figure 5.10. In which, the original image as shown in Figure 10 (a) is standard images such as Lena, with sizes of 512x512 pixels. The watermark uses UCSY logo as shown in Figure 10 (b) with sizes of 256x256 pixels. In the testing, the watermarked image is made filtering 20% of the whole image as shown in Figure 10.(c). The watermark can still be extracted from watermarked image as shown in Figure10.(d). The PSNR value for before filtering attacking is 41.7263dB and the value after attacking is 37.0594 dB.



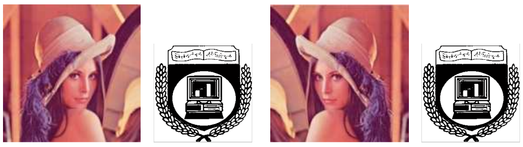
(a) (b) (c) (d)

Figure 10. Robustness to Filtering Attack

3.7.3 Tests and Results of Robustness to Flipping Attack

Another case of image manipulation to test robustness is flipping attack where the effective appearance of the watermarked image has been altered as shown in Figure 11.

The presented system describes that it can manage the robustness issues of image watermaking scheme by extraction the watermark from flipping attacked watermarked image. In which, the original image is standard images such as Lena as shown in Figure 11 (a), sizes of 512x512 pixels. The watermark use UCSY logo as shown in Figure 11 (b) with sizes of 256x256 pixels. In the testing, the watermarked image is made horizontal flipping of the whole image as shown in Figure 11.(c). The watermark can still be extracted from watermarked image as shown in Figure 11.(d). The PSNR value for before horizontal flipping attacking is 41.7263dB and the value after attacking is 37.0989 dB.

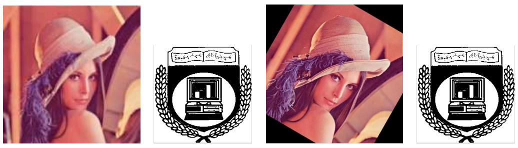


(a) (b) (c) (d)

Figure 11. Robustness to Flipping Attack

3.7.4 Tests and Results of Robustness to Rotation Attack

The watermarked image as shown in Figure 12 (a) can handle the attack of rotation as shown in Figure 12 (c). The watermark can be extracted from the attacked image as shown in Figure 12 (d). The PSNR value for before 30 Degree clockwise direction rotation attack is 41.7263dB and the value after attacking is 29.4909 dB.

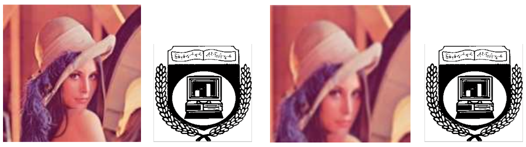


(a) (b) (c) (d)

Figure 12. Robustness to Rotation Attack

3.7.5 Tests and Results of Robustness to Cropping Attack

The watermarked image as shown in Figure 13 (a) can handle the attack of cropping as shown in Figure 13 (b). The watermark can be extracted from the attacked image as shown in Figure 13 (c).



(a) (b) (c) (d)

Figure 13. Robustness to Cropping Attack

3.7.6 PSNR Values over Different Measurements

The results for standard images with in terms of same resolution and same size are in the range of 30dB and 47dB. The sizes of the original image are 512x512 pixels and the watermark sizes are also 512x512 pixels. In this testing, same sizes and same resolution mean that the original image and the watermark are the same, for instance, the original image is Lena with 512x512 pixels and the watermark is also Lena with 512x512 pixels. The PSNR results are shown in Figure 14.

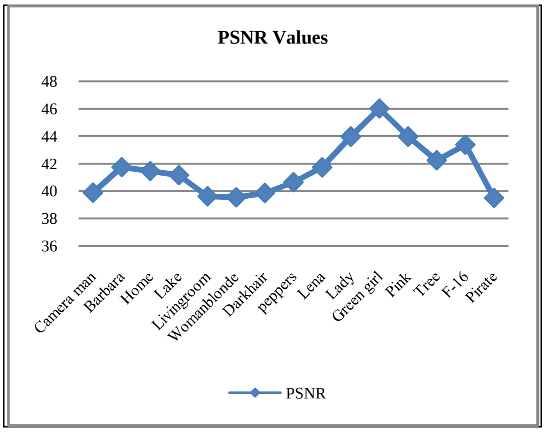


Figure 14. PSNR values over same standard Images

PSNR values for Noise Attack with different amount of noise are described in Figure 15. It is evident that the watermarking scheme can resist noise attack for various percentages. It has PSNR values in the range of 28dB and 34dB. Moreover, extracted watermark is also very strong for robustness when a heavy amount of additional noise is added. For instance, adding 50% Salt and Peppers noise. In the testing, the original image and the watermark image are the same for resolution and sizes

PSNR	5%	15%	25%	50%
Lena	33.1944	30.7773	29.6675	28.1671
Mandrill	33.1994	30.7595	29.6982	28.1912
Peppers	33.0547	30.6509	29.5486	28.0375
Woman Blonde	33.3406	30.9486	29.688	28.3359
Barbara	33.2167	30.8157	29.7127	29.1998
Camera_Man	33.085	30.7195	29.6081	28.1074

Figure 15. PSNR Values Changes over Different Noise Levels

4. Conclusion

In this paper, an approach for copyright protection of digital images using watermarking is presented. Lifting wavelet transform is used to decompose the original image. Discrete cosine transform is applied on the selected LWT sub-bands. The watermark image is embedded in the DCT transformed the selected LWT sub-band of the original image. Subsequently, the watermark image is extracted from the watermarked image. The presened system can handle the main purposes of digital image watermarking such as imperceptibility and robustness. In addition, the robustness issue can be handled against attack such as noise, filtering, flipping, rotation and cropping region of the watermarked image.

References

[1] Chu, W, "DCT-Based Image Watermarking Using Subsampling," IEEE Trans. Multimedia, 5(1): 34-38, 2003.

[2] Deng, F. and B.Wang, 2003. "A novel technique for robust image watermarking in the DCT domain," in Proc of the IEEE 2003 Int. Conf. on Neural Networks and Signal Processing, vol. 2, pp: 1525-1528.

[3] S.S.GONGE, JAGDISH W.BAKAL,"ROBUST DIGITAL WATERMARKING TECHNIQUE BY USING DCT AND SPREAD SPECTRUM", *International Journal of Electrical, Electronics and Data Communication*, ISSN (PRINT): 2320-2084, Volume – 1, Issue – 2, 2013, pp.27-32.

[4] K. Hameed, Adeel Mumtaz, and S.A.M. Gilani , "Digital Image Watermarking in the Wavelet Transform Domain", World Academy of Science, Engineering and Technology, 13 2006, pp.86-89.

[5] M. Jiansheng, L. Sukang and T. Xiaomei, " A Digital Watermarking Algorithm Based On DCT and DWT", *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)*, Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.

[6] Yang Jie," Algorithm of image information hiding based on new anti-Arnold transform and Blending in DCT domain", Communication Technology (ICCT), *2010 12th IEEE International Conference onDigital Object* Identifier: 10.1109/ICCT.2010.5689227, 2010 , pp. 312 - 315, IEEE Conference Publications.

[7] Lin, S. and C. Chin, 2000. "A Robust DCT-based Watermarking for Copyright Protection," IEEE Trans. Consumer Electronics, 46(3): 415-421.

[8] A. Phadikar, S. P. Maity and Malay K. Kundu, "Quantization Based Data Hiding Scheme for Efficient Quality Access Control of Images using DWT via Lifting", in proceedings of Sixth Indian Conference on Computer Vision, Graphics & Image Processing, Bhubaneswar, India, pp: 265- 272, 2008.

[9] Rao, K. and P. Yip. Discrete Cosine Transform: algorithms, advantages, applications. Academic Press, USA, 1990.

[10] Dr. E. Walia , Payal Jain , Navdeep, “An Analysis of LSB & DCT based Steganography”, *Global Journal of Computer Science and Technology,* Page 4, Vol. 10, Issue 1(Ver 1.0), April 2010.

[11] Wu. C and W. Hsieh, "Digital watermarking using zerotree of DCT," IEEE Trans. Consumer Electronics, vol. 46, no. 1, pp: 87-94. 2000.