Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A 2-Level DWT Based Approach for the Implementation of Image Steganography

Priyanka B. Kutade *
Dept. of E&TC, G.H.Raisoni College of Engg. and Management, University of Pune, Maharashtra, India

Parul S. Arora Bhalotra
Asst. Prof., Dept. of E&TC, G.H. Raisoni College of Engg. and Management, University of Pune, Maharashtra, India

Abstract— Steganography is a way of data hiding within images for protected transmission. In recent years, Steganography is important area of research that involves a number of applications. It is an ability of concealing data in a cover image file without causing statistically important any variations to the cover image. In this image steganography, data as secret in the form of image file is concealed within another image as cover with transformations such as integer wavelet transformation, discrete cosine transform, z transformation, Discrete Wavelet Transform etc. This area of research is important more than ever when reliable and secure information exchange is essential. Secret messages are concealed within the high frequency coefficients obtained from Discrete Wavelet Transform.

This system proposes an image Steganography based approach that can confirm the reliability of the data that is being transmitted to receiver. This system presents a novel procedure designed for DWT based Image steganography, where cover image is transformed from spatial domain to frequency domain. In the transform domain approaches, secret messages are implanted in the high frequency coefficients and low frequency sub-band coefficients are preserved unchanged for improving the image quality.

This system Implement and compare 2-level DWT (Discrete Wavelet Transform) approach and DCT (Discrete Cosine Transform) approach For the Implementation of Image Steganography.

Keywords— Image Steganography, Discrete Wavelet Transform, Wavelet, Decomposition, DCT

I. INTRODUCTION

As everyone becomes friendly with the Internet usage so the security of information is important factor in communication. In Cryptography numerous techniques have been created to encrypt and decrypt information in order to maintain the message secret. The purpose is to ensuring the secrecy of communication. Occasionally it is not sufficient to maintain the message contents secret but it is also necessary to keep the existence of message as secret. The procedure to implement this is steganography. The steganography [2], [10] word originated from the Greek words "*stegos*" & "*grafia*" meaning "covered writing". In this approach of image steganography the important data is concealed entirely in images. Steganography is the science and art of invisible communication. This is achieved through concealing important data into another important data, as a result hiding the subsistence of the communicated information.

The majority popular cover objects in steganography are images. Many different image file formats exist in domain of digital images. Different steganographic algorithms exist for these different image file formats.

The basic idea of this paper is that when we decompose an image with DWT, it divides the image in frequency components. Then we get the low & high frequency coefficients. High frequency components are also called as the detailed coefficients which hold the additional information about image and low frequency components are called as approximate coefficients holding almost the original image. These high that is detailed coefficients can be used to hide secret image. This system will take two images, one as cover image and other as secret message. In DWT based image steganography we first perform embedding procedure; cover image is converted in wavelet domain. After this we will modify high frequency coefficients to embed secret image. This secret image further retrieved in extraction procedure to provide the intention of steganography.

II. RELATED WORK

Barnali Gupta et al. [1] have proposed A method for image steganography utilizing basics of discrete wavelet transform. This system maintains secrecy which the prime objective of steganography. It succeeds to maintain the original image unbroken, after the extraction of secret message. This work is related with steganography system using DWT domain. Parul et al. [15] presents the image steganography using discrete wavelet transform. Discrete Wavelet Transform is applied on color images. Then they used Arnold transformation is used to get better security. This paper tries to improve the demerits of earlier related image steganography methods. From the results concluded that this approach is superior in terms of high embedding capacity and PSNR.

Gurmeet Kaur [6] et.al presented paper is based on the comparison of the DWT and DCT [18] method. This paper gave a novel method DWT based Image steganography. As compare to DCT the experimental outcomes confirmation that the DWT based algorithm has a good invisibility & a high capacity. When we have to increase the pay load capacity, DWT method is best. PSNR of original oimage with stego image shows the better results than other existing Steganography approach.

Deqing Sun [25] proposed a method in which they achieves paper in most cases, succeeds higher PSNR gain as compared to further methods and the handled images keep good visual quality. Also, they examined the noise model used and its parameter setting. The noise model undertakes that the obtained DCT coefficients in addition their quantization errors are not dependent.

Po-Yueh Chen* and Hung-Ju Lin [14] proposes A DWT Based Approach for Image Steganography, the low frequency part is kept unaltered as the secret data messages are implanted in the high frequency sub-bands better PSNR is not a surprising result.

H. B. kekre et al. [17] introduces Image using DCT and DCWT in which it gives their comparative study and performance analysis. In both the algorithms each image is divided into 3 planes to form the feature vectors and color data is controlled independently.

Suchitra. B, Priya. M, Raju.J, [3] presents Image Steganography Based On DCT Algorithm for Data Hiding.

A. Discrete Wavelet Transform

A wavelet is a small wave that oscillates and decays in time domain. In computer science, the Discrete Wavelet Transform is a computationally efficient and relatively latest procedure. For both local analysis & multi-resolution analysis the Wavelet analysis is beneficial. Multi-resolution analysis (MRA) is defined as to evaluate a signal at a variety of frequencies with various resolutions. There are two types of Wavelet analysis continuous & discrete. For our system DWT based image steganography uses discrete type. In this system cover image is transforms into wavelet domain, processes the cover image then Inverse DWT is performs to get stego image.

Spatial domain information can be converted to frequency domain information by Wavelet transforms (WT). [4],[5]The Fourier transforms time domain signal into global frequency distributed signal. The Inverse Fourier transform gives original reconstructed signal. The formula for Fourier Transform is as follows:

$$x(t) = \int_{-\infty}^{\infty} X_{FT}(f)e^{-j2\pi ft}df$$

The formula for Inverse Fourier Transform is as follows:

$$X_{FT}(f) = \int_{-\infty}^{\infty} x(t)e^{-j2\pi ft}dt$$

Fourier Transform was first established before the wavelet transform. But the limitation of Fourier Transform is it only gives the frequency distribution of signal. It does not give which frequency with respect to time. So STFT was introduced to overcome the limitations of FT. STFT introduced the Windowing concept. In this the Fourier Transform is applied over the selected window part and it gives the frequency with Time.

The formula for STFT is given as;

$$X_{STFT}(\tau, f) = \int_{-\infty}^{\infty} x(t)g^{*}(t-\tau)e^{-j2\pi ft}dt$$

Wavelet transform is better for local analysis than FT. It can make known signal properties like breakdown points, discontinuities etc. more undoubtedly than FT.

Wavelet contains two orthogonal functions that are father wavelet and mother wavelet. Wavelet basis set begins with the two orthogonal functions: Father wavelet's function is the scaling function and mother wavelet's function ψ(t), is scaling and translation. The formula for Wavelet transform can be given by:

$$F(a,b) = \int_{-\infty}^{\infty} f(x)\varphi^{*}_{(a,b)}(x)dx$$

Where the * denotes the complex conjugate symbol of function ψ called as mother wavelet or wavelet function. The formula for Continuous wavelet transform (CWT) can be given by:

$$X_{WT}(\tau, s) = \frac{1}{\sqrt{|s|}}\int x(t).\varphi^{*}\left(\frac{t-\tau}{s}\right)dt$$

The transformed signal is a function of the scale parameter and translation parameter. ψ denotes the mother wavelet and * indicates it's the complex conjugate. Continuous Wavelet Transform does analysis as a result of contraction and dilation of mother function. Discrete Wavelet Transform uses filter banks to evaluate and rebuild signal. A filter bank divides a signal in various frequency bands. By using following low pass and high pass filters In ***Mallat Tree decomposition***, DWT [9] of a discrete time signal is computed**.** In below figure, the input signal which is image is shown by the x[n], where n is an integer. H0 denotes the high pass filter and L0 denotes the low pass filter. The output of high pass filter is detail coefficients or detail information d[n] and the output of the low pass filter is approximate coefficients a[n]. The input data is passed through set of low pass and high pass filters. The output of low pass filters high pass is downsampled by 2.

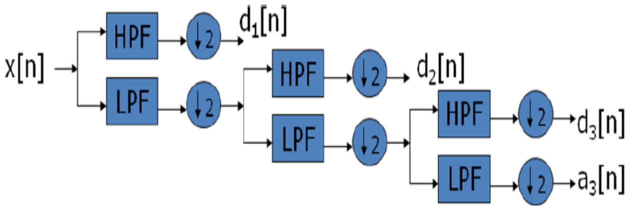

Fig.1 Wavelet decomposition tree (Three-level)

The right side of matrix contains the downsampled high pass coefficients while the left side of matrix contains each row's downsampled low pass coefficients; after applying 2-D DWT as given below in figure,

Fig.2 First stage of step 1 wavelet decomposition

In Next step we apply dwt one step to all columns. Results in four types of coefficients: HH,LH,HL,LL as follows:

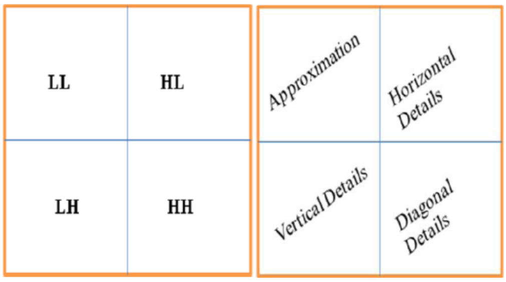

Fig.3 Final stage of step 1 wavelet decomposition

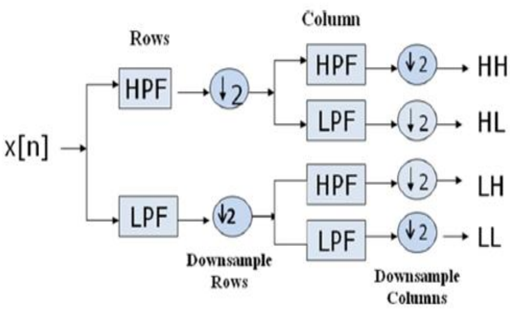

Fig.4 Block diagram of 1 step 2-D DWT

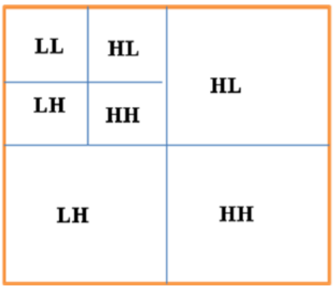

Fig.5 2-step decomposition

B. Discrete Cosine Transform

For JPEG compression Discrete Cosine Transform coefficients are used. It divides the image into sections of different weight. It translates a image or signal from the spatial domain or time domain to the frequency domain. It is capable of split the image into low, middle and high frequency components.

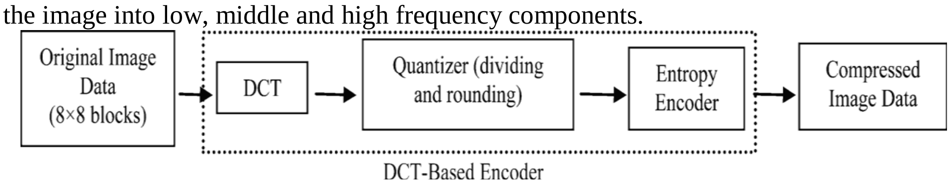

Fig.6 DCT

By applying the two-dimensional DCT to the nonoverlapping and consecutive 8 x 8 blocks of the original image data, the DCT coefficients will be obtained. The obtained coefficients are then fed to the quantizer. In the quantizer, the DCT coefficients are first divided by the steps of quantization and then rounded to obtain the quantized DCT coefficients. At last, the quantized DCT coefficients are entropy encoded to have the compressed image data. For simplicity, the coefficients that divided by steps of quantization and which are not yet rounded are called unrounded DCT coefficients. The coefficients which have been separated by means of the steps of quantization and rounded are referred as quantized DCT coefficients.

In high frequency sub-band, high frequency image components are typically removed by the procedure of compression with noise attacks. In low frequency bands, much of the signal energy lies at low frequency which represents the similar as original image contains most important visual parts. So the secret message is implanted as a result of altering the coefficients in the middle frequency sub-band which resulted as the visibility of the cover image will not be pretentious. The general equation for a 1D DCT is defined by the following equation:

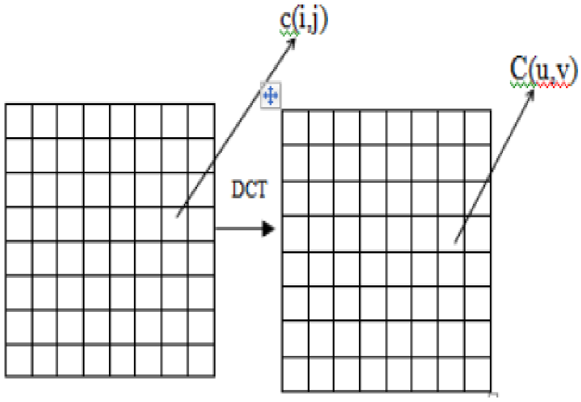

Fig-7 Discrete Cosine Transform of an Image

$$C(u) = a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where, u= 0, 1, 2….. N-1

The equation for a 2D (N x M image) DCT is defined by:

$$C(u,v) = a(v)\sum_{i=0}^{N-1}\left[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)\right] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Where, u , v = 0,1,2….N-1

Here, the input image size =N X M.

C (u, v) = the DCT coefficient with respect to row and column u and v resp. of the DCT matrix.

c (i, j) = With respect to row i and column j the intensity of the pixel.

DCT based steganography Image is divided into 8×8 blocks of pixels. Working from top to bottom, left to right, DCT is applied to each block.

After applying DCT to each block is compressed via quantization table to obtain DCT coefficients furthermore message is implanted in DCT coefficients.

III. IMPLEMENTATION

PROPOSED SYSTEM

A. DCT

In this project, we implement steganography using DCT and steganography using 2 level DWT.

First we implement DCT approach, In that we apply the two-dimensional DCT to the non-overlapping and consecutive 8 x 8 blocks of the original image data, the DCT coefficients will be obtained. The obtained coefficients are then fed to the quantizer. In the quantizer, the DCT coefficients are first divided by quantization steps and then rounded to obtain the quantized DCT coefficients. At last, the quantized DCT coefficients are entropy encoded to have the compressed image data.

Algorithms:

DCT Algorithm for embedding:

1. Read the cover image
2. Calculate the size of cover image
3. Read the secret image
4. Prepare secret message vector
5. Divide the cover image into 8x8 blocks of pixels using DCT quantization.
6. Generate pseudo-random number (Pn) as zero & one.

7. Modify coefficients by adding Pn as zero & one when message bit = 0,1 respectively.
8. Apply inverse DCT
9. Prepare stego image to display

DCT Algorithm for extraction:

1. Load Stego image.
2. Generate pseudo-random number (Pn) as zero & one.
3. Decompose the Stego image using DCT into 8x8 blocks of pixels.
4. Turn the message vector bit to value 0; if the correlation value zero is greater than correlation value one otherwise set to 1.
5. Prepare message vector to display secret image

B. DWT

Then we apply Discrete Wavelet Transform on cover image. It divides the image in time domain to frequency components[1]. Obtained high frequency components represents the detailed coefficients having additional information regarding the cover image and The low frequency components represents approximate coefficients regarding almost same as original image. We will use detailed coefficients to conceal secret image. This system will take an image as cover object in addition to another small image as secret message. In encoding procedure, initially will convert or translate cover image in wavelet (frequency) domain. Later than the translation we alter or manipulate high frequency component for the purpose of secret image data. We retrieved secret image data in extraction process to maintain steganography.

DWT Algorithm for embedding:

1. Load cover image.
2. Determine the size of cover image.
3. Load the secret image.
4. Prepare message vector of secret image.
5. Apply wavelet transform on Cover image.
6. Create (Pn) pseudo-random number.
7. When message bit of secret message vector is 0 by adding Pn, alter detailed coefficients that are vertical and horizontal coefficients of wavelet decomposition.
8. Apply inverse DWT
9. Display the obtained stego image.

DWT Algorithm for extraction:

1. Load the cover image.
2. Load the stego image.
3. Using wavelet transform decompose the cover image and stego image.
4. Create message vector bits of value of all ones.
5. Compute the correlation among the modified coefficients and original coefficients of stego image and cover image respectively.
6. Condition is that correlation values is greater than mean correlation value then convert the message vector bit to 0.
7. Arrange message vector and create display secret image

IV. RESULTS

For the analysis of DWT & DCT based Steganography we have performed experiments. For this we have taken coer image as penguins image of 512*512 pixels .jpg image & 52*19 pixels of .bmp secret image. As shown in fig.8 & fig.9.

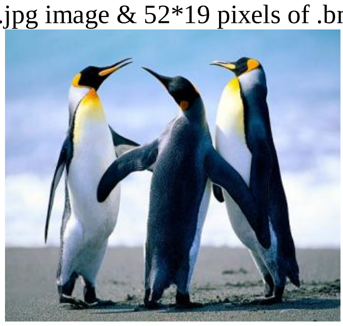

Fig.8 Penguins.jpg as Cover image

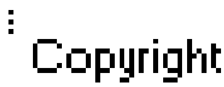

Fig.9 Copyright.bmp as Secret image

For checking the efficiency of algorithms we used matlab 7. The results we have got in terms of GUI as shown in below figures 10., 11, 12. From the results, we displayed Stego-image, extracted secret image, PSNR & MSE values. By comparing GUI of DCT & DWT we conclude that the quality of extracted image & stego image is greater in DWT as compared to DCT based image steganography.

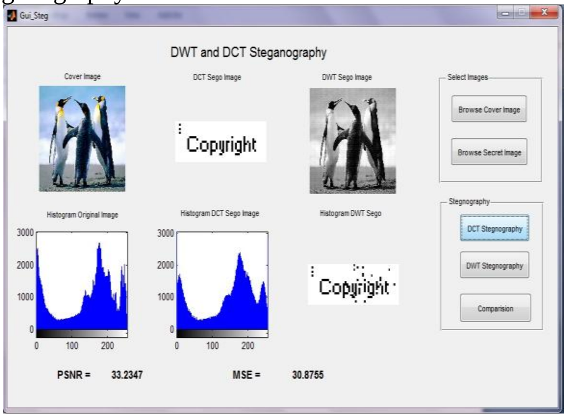

Fig.10 GUI of DCT

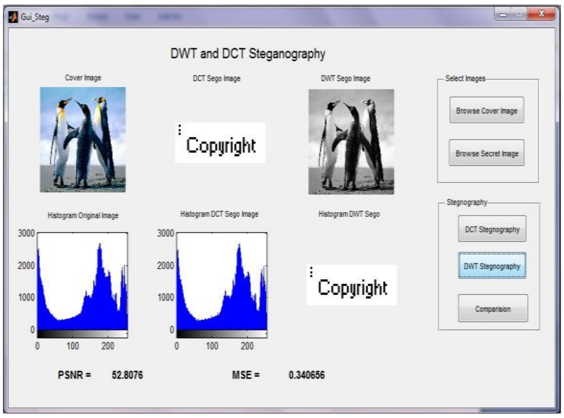

Fig.11 GUI of DWT

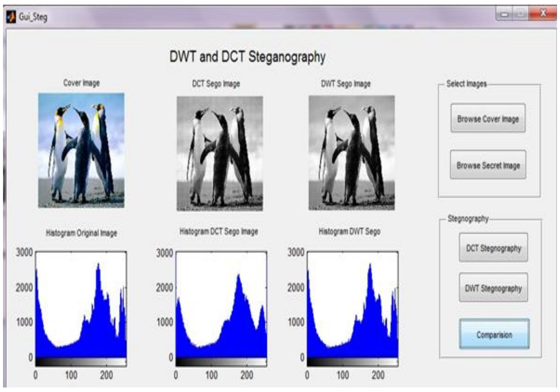

Fig.12 GUI of comparison of DCT & DWT

We have other images as cover & secret image. For these images we calculated PSNR & MSE values. The results we achieved with the help of MATLAB 7 ate shown in below Table 1.

  

Fig.13 Lena.jpg of 512*512 pixels of image as Cover image
Fig.14 Flower.jpg of 512*512 pixels of image as Cover image
Fig.15 Copyright2.bmp of 52*19 pixels of image as secret image

TABLE I PSNR & MSE VALUES FOR DCT & DWT BASED IMAGE STEGANOGRAPHY

METHOD	COVER IMAGE	SECRET IMAGE	PSNR	MSE
DCT	Penguins	Copyright	33.234	30.875
DWT	Penguins	Copyright	52.807	0.340
DCT	Flower	Copyright	33.188	31.205
DWT	Flower	Copyright	52.815	0.340
DCT	Lena	Copyright	33.079	31.999
DWT	Lena	Copyright	52.800	0.341
DCT	Penguins	CS	33.244	30.205
DWT	Penguins	CS	53.915	0.263
DCT	Flower	CS	33.195	31.156
DWT	Flower	CS	53.921	0.263
DCT	Lena	CS	33.088	31.933
DWT	Lena	CS	53.908	0.264

From the above table if we check the values for PSNR of DWT algorithm are better than DCT algorithm. So we conclude that for the display quality of stego image & extracted image is better in DWT based image steganography than DCT based image steganography.

V. CONCLUSION

Steganography is the fine art and skill of undetectable communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. We have implemented DWT & DCT based image Steganography approaches and compared the results in terms of Stego images, Extracted images. We calculated PSNR & MSE values. From the results, conclusion can be drawn that the DWT based approach for Image steganography is superior in terms of PSNR & MSE than DCT.

ACKNOWLEDGEMENT

I would like to say thanks to my guide "Prof. Parul S. Arora Bhalotra" who gave her knowledge and time in order to complete this paper. This paper would never complete without her and the support of faculty members.

REFERENCES

[1] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, "A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013, ISSN: 2277 128X

[2] T Morkel, MS Olivier and JHP Eloff, "An Overview of Image Steganography," (ISSA2005), in Proceedings of the Fifth Annual Information Security South Africa Conference Sandton, South Africa, (Published electronically) June/July 2005

[3] M, Raju, B, Priya, Suchitra, "Image Steganography Based On DCT Algorithm for Data Hiding", (IJARCET) International Journal of Advanced Research in Computer Engineering & Technology Volume 2, Issue 11, November 2013 3003

[4] Nilam N Ghuge, Parul S Arora Bhalotra, B. D. Shinde, "CBIR using Textural Feature", International Journal of Computer Applications, Volume 56– No.11, October 2012

[5] Nilam N Ghuge, Parul S Arora Bhalotra, B. D. Shinde,"Shot Boundary Detection for a Video under the Influence of Illumination: A Adaptive Thresholding Approach, International Journal of Computer Applications, Volume 56– No.11, October 2012

[6] Rupinder Kaur, Mandeep Kaur, Rahul Malhotra, " A New Efficient Approach towards Steganography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (2) , 2011, 673-676

[7] Adnan Abdul-Aziz and Gutub Mohammad Tanvir Parvez, "RGB Intensity Based Variable-Bits Image Steganography", IEEE Asia-Pacific Services Computing Conference 2008

[8] LinjieGuo, Student Member, IEEE, Jiangqun Ni, Member, IEEE, and Yun Qing Shi, Fellow, IEEE, "Uniform Embedding for Efficient JPEG Steganography", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 5, May 2014

[9] Parul S. Arora Bhalotra, Bhushan D. Patil, "Shot Boundary Detection using Radon Projection Method" ACEEE Int. J. on Signal and Image Processing , Vol. 4, No. 3, Sept 2013

[10] Priyanka B. Kutade, Parul S. Arora Bhalotra, "A Survey on Various Approaches of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 3, January 2015

[11] A.A.Al-Saffar , "Proposed Steganography Method Based on DCT Coefficients", IBN AL- HAITHAM J. FOR PURE & APPL. SCI. VOL.24 (3) 2011

[12] Jiri Fridrich, "A New Steganographic Method for Palette-Based Images", Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902-6000

[13] Surbhi Gupta, Parvinder S. Sandhu, “Exploiting the RGB Intensity Values to Implement a Novel Dynamic Steganography Scheme”, International Journal of Research in Engineering and Technology (IJRET) Vol. 2, No. 4, 2013 ISSN 2277 – 4378

[14] Hung-Ju Lin, Po-Yueh Chen, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 2006.

[15] Dr. Harish Rohil, Parul1, Manju2, “Optimized Image Steganography using Discrete Wavelet Transform (DWT)”, International Journal of Recent Development in Engineering and Technology, ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014

[16] Er. Rohini Sharma, Er. Mahender Singh, Er. Dinesh Garg, “ A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[17] H. B. kekre and Kavita Sonawane, “Retrieval of Images Using DCT and DCT Wavelet Over Image Blocks”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 10, 2011

[18] Parul S. Arora Bhalotra, Bhushan D. Patil, “Video Segmentation Using Radon Projection and Ridgelet Transform: A Comparative Analyasis”, ELSEVIER Int. Conf. on Applied Information And Communication Technology 2014.

[19] Deepak Singla1, Rupali Syal2, “Data Security Using LSB & DCT Steganography In Images”, International Journal Of Computational Engineering Research/ ISSN: 2250–3005

[20] B.Padmasri, M.Amutha surabi, “Spread Spectrum Image Steganography with Advanced Encryption Key Implementation”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013 ISSN: 2277 128X

[21] Ankit Gupta, Rahul Garg, “Detecting LSB Steganography in Images”

[22] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, “ Implementation of Image Steganography Using 2-Level DWT Technique”, International Journal of Computer Science and Business Informatics

[23] Ajit Danti, Preethi Acharya, “Randomized Embedding Scheme Based on DCT Coefficients for Image Steganography”, IJCA Special Issue on “Recent Trends in Image Processing and Pattern Recognition” RTIPPR, 2010.

[24] S. S. Nassar, N.M.Ayad, M.H. Kelash, O. S., M. A. M. El-Bendary, “Image Contents Verification Algorithm using Transform Domain Techniques” International Journal of Computer Applications (0975 – 8887) Volume 97– No.9, July 2014

[25] Deqing Sun, Student Member, IEEE, and Wai-Kuen Cham, Student Member, IEEE, “Postprocessing of Low Bit-Rate Block DCT Coded Images Based on a Fields of Experts Prior”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 16, NO. 11, NOVEMBER 2007

