Hybrid DWT- DCT image steganography for encrypted secret image

ARCHANA O. VYAS[1], Dr. SANJAY V. DUDUL[2]
Department of Applied Electronics
SantGadge Baba Amravati University
Amravati, Maharashtra
INDIA
nyasa.archana@gmail.com[1],svdudul@gmail.com[2]

Abstract: -Steganography is the science of hiding secret information in any cover medium like image or video, for the purpose of secure transmission. However, steganography ensures protection of data by hiding it in a cover object. Moreover, cryptography along with steganography, ensures security in depth. Cryptography is the technique of encrypting the original information using a key. Challenging aspects in Image steganography are to increase the payload capacity of secret information and robustness against visual attacks and statistical attacks. The combined technique of DWT and DCT provides advantages of both techniques. The proposed technique of image steganography provides higher robustness against statistical attacks, higher imperceptibility. This technique is more secure as the encrypted secret image is hidden in two cover images, with prior application of DWT and DCT on both cover images. The simulation results illustrate the high embedding capacity and reasonable PSNR values.

Key-Words: -Steganography, Cryptography, DWT, DCT, PSNR, MSE

1 Introduction

Steganography is the art of concealing the existence of information within seemingly harmless carriers. Steganography can be viewed as similar to cryptography. Both have been used as means to protect information. At times, these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages, so if intercepted, the messages cannot be understood. Steganography, in an essence, "masks" a message to hide its existence and makes it seem "invisible" thus concealing the fact that a message is being sent altogether [1]. Images are the most popular choice as cover media for steganography. Steganography schemes developed so far can be categorized as spatial domain and transform domain. Spatial Domain Techniques constitute bitwise manipulation of intensity of pixels. There are various approaches to embed data in spatial domain. Most commonly used and simple techniques for spatial domain are Least Significant Bit (LSB) Methods and pixel Value Differencing (PVD) method. LSB includes replacing least significant bits of cover object with secret image or data. It is the most popular and simple technique when dealing with images. It has low computational complexity and high embedding capacity[2]. Number of insertion bits in PVD depends on whether the pixel is an edge or a smooth area. Human Visual System is sensitive to subtle changes in the smooth areas as compared to the edges. This is mainly because the difference between pixels in the smooth areas is much less as compared to that between the edge pixels and embedding in edge pixels results less visual distortion. PVD does not cause much visual distortion and neither it is directly vulnerable to the histogram attack as the LSB substitution. It is however susceptible to histogram analysis of the differences of the pixel pairs and $\chi 2$-attack [3].Transform domain techniques are also known as frequency domain techniques.Transform domain techniques first convert image from spatial domain to frequency domain and then secret message is embedded. These techniques hide data by using mathematical functions. In Frequency domain schemes, the secret data will be embedded into transform coefficients which are transformed firstly in to frequency domain by various frequency domain methods like Discrete Cosine Transformation (DCT), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), etc. Secondly secret data will be embedded into transform coefficients [3].

1.1 Discrete Cosine Transform

Most commonly used transform domain technique is Discrete Cosine Transform (DCT). It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into

high, middle and low frequency components [4].In low frequency sub-band, much of the signal energy lies at low frequency, which contains most important visual parts of the image. While in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. DCT is used in steganography as Image is split into 8×8 blocks of pixels. Embedding in DCT domain is simply accomplished by altering the DCT coefficients. DCT transformation and compression using quantization and run-length coding on raw images can be used to obtain secure stego images [5].

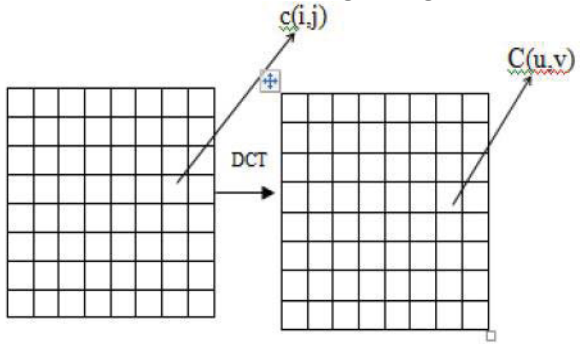

Fig. 1 Discrete Cosine Transform

Let I(x,y) denote an 8-bit gray scale cover-image with x = 1,2,…….,M_1 and y = 1,2,…….,N_1. This $M_1 \times N_1$ cover-image is divided into 8 × 8 blocks and two-dimensional (2-D) DCT is performed on each of L =$M_1 \times N_1$ / 64 blocks. The mathematical definition of DCT is [6]:
Forward DCT:

$$F = (u,v) = \frac{1}{4} C(u)C(v) \sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) Cos\,[\{\pi(2x+1)u\}/16]\, Cos\,[\{\pi(2y+1)v\}/16] \quad \text{..... (1)}$$

For$u$ = 0,...,7 and$v$ = 0,...,7

Where,

$$C(K) = \begin{cases} \frac{1}{\sqrt{2}} & for\ k = 0 \\ 1 & otherwise \end{cases} \quad \text{…….. (2)}$$

Inverse DCT:

$$f = (x,y) = \frac{1}{4} \sum_{u=0}^{7} \sum_{v=0}^{7} C(u)C(v)F(u,v) Cos\,[\{\pi(2x+1)u\}/16]\, Cos\,[\{\pi(2y+1)v\}/16] \quad \text{..... (3)}$$

For$x$ = 0,...,7 and$y$ = 0,...,7 [6]

As shown in the Fig. 1 C (u,v) is the DCT coefficient in row u and column v of the DCT matrix, c(i,j) is the intensity of the pixel in row i and column j of the image.

1.2 Discrete Wavelet Transform

DWT transforms discrete signal from time domain to frequency domain i.e., it provides both time and frequency representation of the signal. The signal to be decomposed is analyzed at different frequency bands with different resolution. The decomposition takes place by transmitting the signal to series of HPF and LPF [7].

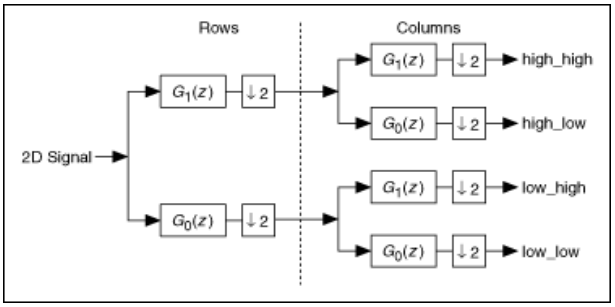

Fig. 2 DWT Decomposition Tree

1.2.1 Haar Wavelet

This was the first and most widely used wavelet. A Haar Wavelet is a certain sequence of rescaled "square-shaped" function which together forms a wavelet family or basis[7]. The Haar wavelet's mother wavelet function $\psi(t)$ can be described as

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2 \\ -1 & \frac{1}{2} \le t < 1 \\ 0 & otherwise \end{cases} \quad \text{…….. (4)}$$

Scaling function of Haar Wavelet is,

$$\Phi(t) = \begin{cases} 1 & 0 \le t < 1 \\ 0 & otherwise \end{cases} \quad \text{..... (5)}$$

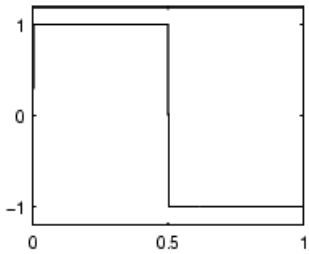

Fig. 3 Haar Wavelet Function Waveform

The two - dimensional Haar-Discrete wavelet transform consists of two operations: One is the horizontal operation and the other is the vertical

one. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as shown in Fig. 4. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L)while the pixel differences represent the highfrequency part of the original image (denoted as symbol H) [8].

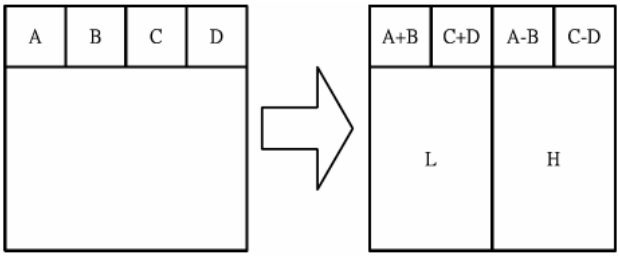

Fig. 4. The horizontal operation on the first row

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Fig.5. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HHrespectively. The LL sub-band is the low frequency portion and hence looks very similarto the original image [8].

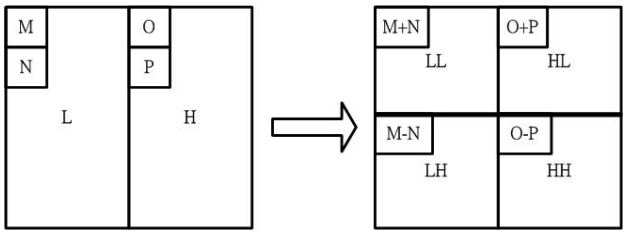

Fig. 5. The vertical operation

After each transform is performed the size of the square containing the most important information is reduced bya factor of 4 as seen in Fig.6 [9].

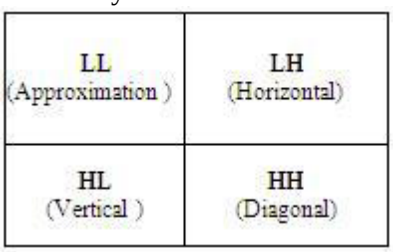

Fig. 6: Detailed 2D Haar Wavelet Transform

2 Reviewed Literature

McKeon [10] reported a methodology for steganography based on Fourier domain of an image by using the properties of zero-padding. These zeros can be changed slightly where the change in the image is not noticeable. In [11], authors discussed the effects of steganography in different image formats and DWT. They also introduced the number of payload bits and the place to embed. In [12], authors proposed method to spread hidden information within encrypted image data randomly based on the secret key. Tsai et al. [13] divided the image into blocks where residual image was calculated using linear prediction. Then, the secret data was embedded into the residual values, followed by block reconstruction. Chao et al. [14] suggested the embedding scheme that hides secret messages in the vertices of 3D polygen models. Li et al. [15] proposed lossless data hiding using difference value of adjacent pixels instead of the whole image. LIU Tong and QIU Zheng-ding [16] and Vladimir Banoci*et al*. proposed a DWT based color image steganography method. In the former method, the secret information is hidden into a publicly accessed color image by a quantization-based strategy. Whereas, the latter method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete transform for embedding process. Ali Al- Ataby [17] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. T. Narasimmalou [18] proposed a new image data hiding technique based on discrete wavelet transform.T. Narasimmalou[19], presented an optimal discrete wavelet transform (DWT) based steganography. Experiments justify that the peak signal noise ratio (PSNR) generated by the proposed method is better.In [20], Liu Lung et al. proposed ajpeg steganographic technique using complementary embedding technique; this method is achieved by dividing the quantized DCT coefficients and the secret bits into two parts according to apredefined partition ratio.

3 Proposed embedding algorithm

To achieve better imperceptibility with robustness and to have a higher PSNR value, we have applied a combined DWT – DCT steganography technique in the proposed work. DWT is applied on two distinct cover images to obtain Coefficients of HH sub band. Before embedding an encrypted secret image in it, the DCT is applied on these sub band DWT

coefficients. Suppose C_1 and C_2 be cover image of size $M_C x N_C$.

$C_1 = \{x_{i,j} | 1 \leq i \leq M_c, 1 \leq j \leq N_c , x_{i,j} \epsilon \{1,2,...255\}$...(6)

$C_2 = \{y_{i,j} | 1 \leq i \leq M_c, 1 \leq j \leq N_c , y_{i,j} \epsilon \{1,2,...255\}$...(7)

The embedding procedure is described in the following steps:

- Read the cover images C_1 and C_2, from the image data base.
- Read the secret image S, to be embedded, from the image data base.
- Show the two cover images and the Secret image on the GUI.
- Calculate the hiding capacity of both coverimages C_1, C_2 and display its value on designed GUI.
- Choose a proper key and encrypt the secretimage S, before embedding it into coverimages using that key, display the encrypted secret image on designed GUI.
- Apply the Discrete Wavelet Transform on the two cover images and get the four sub-bands LL, HL, LH and HH per cover image.
- Correlate the encrypted secret image size with HH sub band size of C_1 and C_2.
- Convert the encrypted secret image, to be embedded in cover image, into binary format.
- Convert HH sub-band of cover image to 8*8 block, it is termed as HH_1 for C_1 and HH_2 for C_2.
- Take one block of 8*8 from HH_1;Perform Discrete Cosine Transform at 8x8 block level, to transform it into 8*8 matrix of DCT coefficients. Exchange the coefficients of block position (5, 2) and (4, 3) on the basis of secret image bit 0 or 1.
- Apply the above step for HH_2 which belongs to cover image C_2.
- Apply Inverse Discrete Cosine Transform on above 8*8 block, place this new block into HH_1 and HH_2 respectively.
- Apply Inverse Discrete Wavelet Transform on altered HH_1 and HH_2 coefficients to get the stego image.
- Show the two stego images on GUI.
- Calculate the mentioned performance parameter values and display on GUI.

4 Proposed extraction algorithm

To retrieve the embedded secret image from the Stego image, the extraction algorithm is described in the following steps.

- Read the stego image SC_1 from the embedded image file and display it on the designed GUI.
- Read the stego image SC_2 from the embedded image file and display it on the designed GUI.
- Select the same key for decryption, as that of encryption of the secret image E, so that the secret image can be obtained in its original form after de-embedding.Write the key on GUI.
- Discrete Wavelet Transformation is applied on two stego images for decomposing into sub-bands i.e. LL, HL, LH, and HH respectively.
- Divide the sub-band HH in 8x8 blocks.
- Reconstruct the secret image using extracted bits from above processed stego images blocks. This obtained image, required to be decrypted now.
- Decrypt the above obtained image using the same key as that of encryption.
- Finally the de-embedded, decrypted recovered original secret image is displayed on the designed GUI.

5 Performance Parameters

The performance parameters that are required to be evaluated after DWT-DCT image steganography are explained as follows.

5.1 Peak-Signal-to-Noise Ratio (PSNR)

Imperceptibility: Imperceptibility means that the distortion or changes in quality of the cover image due to embedding of secret image should not be perceived. The imperceptibility is measured mathematically in terms of Peak signal to noise ratio (PSNR). PSNR is defined as below.

$$PSNR = 10\ log_{10}(\frac{255^2}{MSE})dB \quad \text{..... (8)}$$

Where MSE denotes Mean Square Error, which is given in equation (9),

$$MSE = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(X_{ij} - Y_{ij})^2 \quad \text{..... (9)}$$

MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. Where *i* and *j* denote the image coordinates, *m* and *n* are the dimensions of the image, *Yij* is the generated stego image and *Xij* is the cover image. PSNR is often expressed on a logarithmic scale in decibels (dB). A higher PSNR

value indicates that the stego image closely resembles the original image. Generally, if PSNR value is greater than 35 dB, the embedded image is within acceptable degradation level and the secret image will be invisible to human visual system [21].

5.2 Hiding Capacity or Payload Capacity

Payload Capacity is amount of data of cover image which is possible to embed with secret information. It can also be defined as maximum number of bits that can be embedded in a given cover image. It is considered as the amount of information that can be hidden within the cover image without deteriorating the quality of cover image. It is given in bits or kilobits [21].

6 Experimental Results

The proposed algorithm is tested in MATLAB programming environment. Fig. 7 depicts the various secret images that are converted to gray image before embedding it, in two cover images.

Fig.7. various secret images: Water melon, Logo, Rose

Fig.8. various cover images: Baboon, Cat, Girl, Lena, Pepper, Fruit

Fig. 7 shows the various secret images and Fig. 8 shows the various cover images used for experimental purpose. Fig. 9(a) shows a GUI that is used to select two cover images of “baboon”, “cat” and secret image “watermelon” from the image database. It shows the encryption of secret image “Watermelon”. It also shows the two stego images obtained after embedding encrypted secret image in two aforementioned cover images. The chosen encryption key is displayed on GUI. The PSNR, MSE during embedding process and hiding capacity of the two cover images are also evaluated and displayed on GUI.

Fig. 9 (b) depicts a GUI that is used to show the two stego images “baboon” and “cat” and same two cover images. There is hardly any difference in the original cover images and the stego images; it indicates that image quality is not degraded after embedding a secret image “water melon” in two cover images. When the same key as that of encryption key is used, the GUI shows the recovered original image “Water melon”. This indicates the faithful recovery of actual secret image without any loss in image content.

Fig. 10 (a) and Fig. 10 (b) demonstrated the experimental results for the secret image “Logo”. Fig.11 (a) and Fig.11 (b) demonstrated the experimental results for the secret image “Rose”. For these secret images, the parameters such as MSE and PSNR are evaluated for embedding as well as de-embedding process; and hiding capacity values in bits for two cover images are displayed on GUI. PSNR in dB, MSE and hiding capacity (HC) in bits for the tested secret images for corresponding cover images displayed in Fig.9, Fig.10 and Fig.11 are as depicted in Table 1.

Table 1 MSE, PSNR and Hiding capacity for DWT - DCT steganography on two cover images during embedding a secret image.

Secret Image	Cover Image 1			Cover Image 2		
Water melon	Baboon			Cat		
	MSE	PSNR	HC	MSE	PSNR	HC
	0.7533	49.36	1048	0.7413	49.43	1433
Logo	Girl			Lena		
	MSE	PSNR	HC	MSE	PSNR	HC
	0.7708	49.26	1566	0.7758	49.23	1048
Rose	Pepper			Fruit		
	MSE	PSNR	HC	MSE	PSNR	HC
	0.7568	49.34	1048	0.7645	49.29	1048

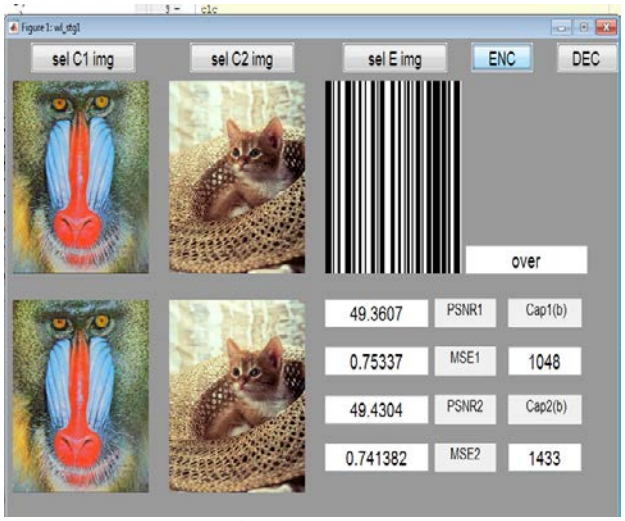

Fig.9(a) Encrypted image of water melon, two cover images & DWT-DCT stego images

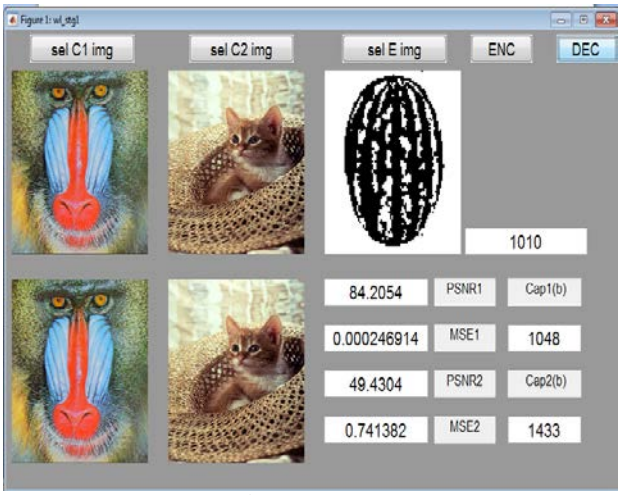

Fig.9 (b) Recovered image of Water melon, two cover images & corresponding DWT-DCT stego images

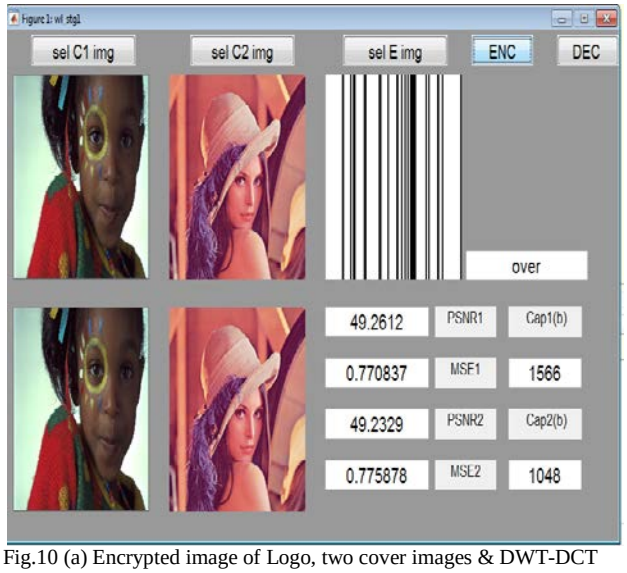

Fig.10 (a) Encrypted image of Logo, two cover images & DWT-DCT stego images

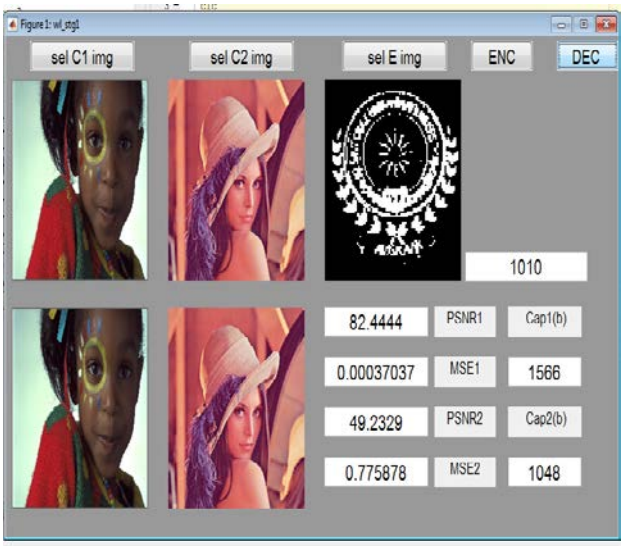

Fig. 10 (b) Recovered image of Logo, two cover images & corresponding DWT - DCT stego images

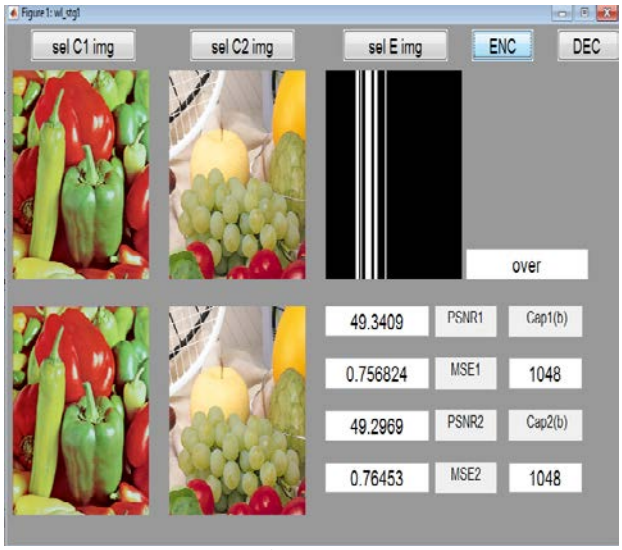

Fig. 11 (a) Encrypted image of Rose, two cover images & DWT-DCT stego images

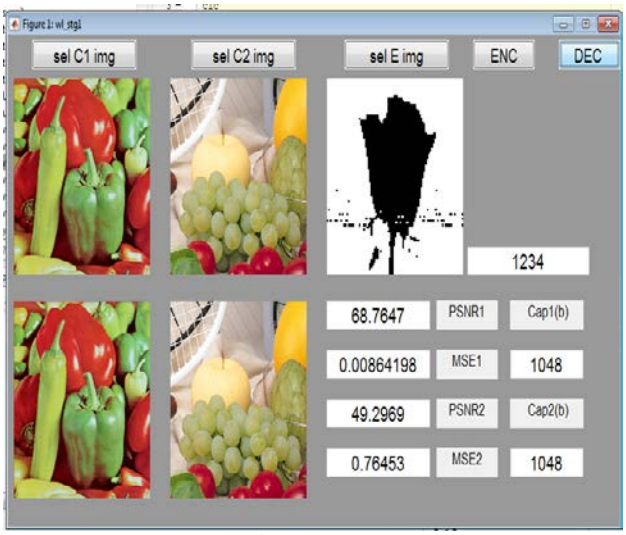

Fig.11 (b) Recovered image of Rose , two cover images & corresponding DWT - DCT stego images

The experiment is conducted over a database of 100 images and it is observed that PSNR values obtained is around 50dB during embedding, thus exhibiting satisfactory quality of images without significant loss of information. PSNR value "49.23 dB" is observed for the cover image "Lena" for corresponding secret image "logo" which is highest among the previously reported methods used by the other researchers. The comparative analysis of DWT – DCT steganography with the prior reviewed work for the cover image "Lena" and corresponding secret image "Logo" is as depicted in Table 2.

Table 2 PSNR value comparison for cover image "Lena" and secret image "logo" between proposed work and previous reported work.

Cover Image	Secret Image	Method	PSNR value in dB
Lena	Logo	Vijay K. Ahire [22]	39.2
		V. Kumar and D. Kumar [23]	41.9
		Gosawi and S. Khandelwal [21]	44
		Proposed Method	49.23

7 Conclusion

A novel method has been implemented to hide the encrypted secret image in two distinct cover images using hybrid DWT-DCT setganography technique. The implementation is on two colour cover images. The method is rigorously tested on a database of 100 images and PSNR value obtained is around 50dB, which is more than the earlier reported PSNR values, so far. The method is found successful with different encryption key on secret images applied on secret image to hide it in two cover images. We have successfully recovered the hidden image using the same key for decryption. A satisfactory high payload capacity of 1566 bits is thus observed. Use of two cover images and encryption before embedding has certainly enhanced the hiding capacity and security of the system as compared to the reported methods applied on a single cover image in the literature.

References:

[1] Gabriel Bugár, VladimírBánoci, Blind Steganography based on 2D Haar Transform, 55th International Symposium ELMAR-2013, 25-27 September 2013.

[2] SumeetKaur ,Talwandi Sabo, Steganography and Classification of ImageSteganography Techniques, IEEE, International conference on computing for sustainable global development (INDIACOM), March 2014.

[3] Ratnakirti Roy, SuvamoyChangder, Evaluating Image Steganography Techniques: FutureResearch Challenges, IEEE, International conference on computing management and telecommunication 978, Jan 2013.

[4] N.F. Johnson and S. Jajodia, ExploringSteganography: Seeing the Unseen Steganography, IEEE transactions on computers, vol. 32, issue 2, Feb. 1998.

[5]Monika Gunjal, Jasmine Jha, Image Steganography Using Discrete CosineTransform (DCT) and Blowfish Algorithm, International Journal of Computer Trends and Technology (IJCTT), volume 11, number 4, May 2014.

[6] A.Nag, S. Biswas, A novel technique for image steganography based on Block-DCT and Huffman Encoding, International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[7] Abhinav Dixit, SwatilekhaMajumdar, Comparative analysis of coiflet and daubechies wavelets using global threshold for image de-noising, International Journal of Advances in Engineering and Technology, ©IJAET ISSN: 22311963, Nov. 2013.

[8] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering, ISSN 1727-2394, 2006.

[9] Essam H. Houssein, Mona A. S. Ali, An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System, Proceedings of the Federated Conference on Computer Science and Information Systems pp. 641–644, DOI: 10.15439/2016F521, ACSIS, Vol. 8, ISSN 2300-5963, 2016.

[10] McKeon, R.T, Steganography Using the Fourier Transform and Zero-Padding Aliasing Properties, IEEE International Conference on Electro/Information Technology, pp.492–497 (2006)

[11] Mastronadri, G., Castellano, M., Steganography Effects in various Formats of Images-A preliminary study, International Workshop on Intelligent Data Acquisition and Advanced Computing Systems Technology and Applications, pp. 116–119 (2001)

[12]. Younes, M.B., Jantan, A., A New Steganography approach for image encryption exchangeby using the Least Significant Bit

Insertion, International Journal of Computer Scienceand Network Security, Vol.8, No.6, 8247–253, June 2008.
[13] Tsai, P., Hu, Y.C., Reversible image hiding scheme using predictive coding and histogram shifting, ACM Journal ofSignal Processing, vol. 89, issue 6, 1129–1143, June 2009.
[14] Chao, M.W., Lin, C.H., A high capacity 3D steganography algorithm, IEEE Transactions on Visualization and computer Graphics, 15(2), 274–284, 2009.
[15] Li, Z., Chen, X., Lossless data hiding scheme based on adjacent pixel difference, International Conference on Computer Engineering and Technology, pp. 588–592, 2009.
[16] T. Liu, Z. Qiu, A DWT-Based Color Image Steganography Scheme, In Proceeding IEEE, 6th International Conference on Signal Processing, vol. 2, pp. 1568-1571, 2002.
[17] Ali Al-Ataby, Fawzi Al-Naima, A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[18] T.Narasimmalou, Allen Joseph R, Optimized Discrete Wavelet Transform based Steganography,IEEE, InternationalConferenceon Advanced CommunicationControland ComputingTechnologies(ICACCCT),2012.
[19] T. Narasimmalou, Allen Joseph R, Discrete Wavelet Transform Based Steganography for Transmitting Images, IEEE, International Conference On Advances In Engineering, Science And Management (lCAESM), 370, March 30, 2012.
[20] C.-L. Liu, S.-R. Liao, High-performance jpeg steganography using complementary embedding strategy, ACM Journal of Pattern Recognition, vol. 41, issue 09, pp. 2945–2955, Sept. 2008.
[21]AnuradhaGoswami, SarikaKhandelwal, Hybrid DCT-DWT Digital Image Steganography, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 6, June 2016.
[22] Vijaya K. Ahire, VivekKshirsagar, Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images, International Journal of Computer Science and Network Security (IJCSNS) VOL.11 No.8, August 2011.
[23] Vijay Kumar, Dinesh Kumar, Digital image steganography based on combination of DCT and DWT, International conference on advances in information and communication technologies pp. 596–601, © Springer-verlag Berlin Heidelberg, 2010