International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014)

Optimized Image Steganography using Discrete Wavelet Transform (DWT)

Parul[1], Manju[2], Dr. Harish Rohil[3]

[1]M.Tech. Scholar, [3]Asst. Professor, Department of Computer Science and Applications, Ch. Devi lal University, Sirsa-125055, Haryana (India)

[2]Department of Computer Engineering, CDL Govt. Polytechnic ES, Nathusari Chopta, Sirsa- 125055

***Abstract*--Steganography is a term used for covered writing. Steganography can be applied on different file formats, such as audio, video, text, image etc. In image steganography, data in the form of image is hidden under some image by using transformations such as z-transformation, integer wavelet transformation, DWT etc and then sent to the destination. At the destination, the data is extracted from the cover image using the inverse transformation. This paper presents a new approach for image steganography using DWT. The cover image is divided into higher and lower frequency sub-bands and data is embedded into higher frequency sub-bands. Arnold Transformation is used to increase the security. The proposed approach is implemented in MATLAB 7.0 and evaluated on the basis of PSNR, capacity and correlation. The proposed approach results in high capacity image steganography as compared to existing approaches.**

***Keywords*-- Image Steganography, PSNR, Discrete Wavelet Transform.**

I. Introduction

The word *steganography* is of Greek origin and means "concealed writing" from the Greek words *steganos* meaning "covered ", and *graphei* meaning “writing”. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message.. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Image Steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image domain also known as spatial domain techniques; embed messages in the intensity of the pixels directly [15]. In transform domain; also known as frequency domain, images are first transformed and then the message is embedded in the image.

Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems”. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format. Steganography in the transform domain involves the manipulation of algorithms and image transforms.

II. Related Work

Steganography is rapidly growing field of research. In the past years, so many papers have been published in the field of image steganography. Anjali *et al.* used *DWT* based approach for steganography using Biometrics. In that, skin region of images is used in *DWT* domain for embedding secret data and image cropping concept introduced to maintain security. Results are shown in the form of table of capacity and PSNR with highest PSNR (53.0 dB) and highest capacity 71% [1]. M.F. Tolba, *et al.* proposed a method for embedding message bit stream into the *LSB*’s of Integer Wavelet Co-efficient of a true color image. Cover image is adjusted before applying Integer Wavelet Transformation (*IWT*) followed by *DWT* (two levels). Results are shown in form of stego image with *PSNR* (73.91 dB). With data rate 1 bpp [4]. Po-Yueh Chen, *et al.* proposed a method, that hide data in high frequency domain resulted from Discrete Wavelet Transformation. Some basic pre-processing methods are applied before embedding. Author divides the algorithm in two modes and three cases. For fix mode 46.83 dB is the highest *PSNR* value and 39.00 dB is lowest. For varying mod highest *PSNR* is 50.85 dB and minimum is 44.76 dB [5].

Ali Al-Ataby, *et al.* proposed a technique that depends on wavelet transform and Information-Hiding System. He used wavelet decomposition for hiding the data [6]. Amitava Nag, *et al.* Proposed a method for steganography based on *DWT*. Data is embedded in High frequency sub band. Two different pseudo random 2D sequences are generated by the session based key. An amplification factor is used to control the embedding effect [7]. K B Shiva Kumar, *et al.* proposed an image steganography strategy based on affine transformation, which can hold up the histogram analysis.

An affine transformation is any transformation that preserves co-linearity and ratios of distances, for example scale, translation, and rotation [8]. K B Shiva Kumar, *et al.* presented a novel technique for image steganography which belongs to techniques taking advantage of sharp areas of image to hide a large amount of secrete data and used a hybrid edge detector is used for that purpose. He combined two techniques in order to produce a new steganographic algorithm. Author used Sobel filter and Laplacian filter on second order derivative of image. Results are shown in the form of stego image *PSNR* (maximum 46.88 dB) and *MSE*. Maximum capacity is 1.89 bpp [9]. A Comparison of proposed approach with various existing approaches is shown in Table 2.

III. Discrete Wavelet Transform

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. Discrete Wavelet Transformation has its own excellent space frequency localization property [7]. The *DWT* splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts.

The high frequency components are usually used for steganography since the human eye is less sensitive to changes in edges [16]. In two dimensional applications, for each level of decompositions, we first perform the *DWT* in the vertical direction, followed by the *DWT* in the horizontal direction. As we can see in Fig.1, after the first level of decomposition, there are four sub-bands: LL1, LH1, HL1 and HH1. For each successive level of decomposition, the LL sub-bands of the previous level is used as the input. To perform second level decomposition, the *DWT* is applied to LL1 band which decomposes the LL1 band into four sub-bands: LL2, LH2, HL2 and HH2 [6].

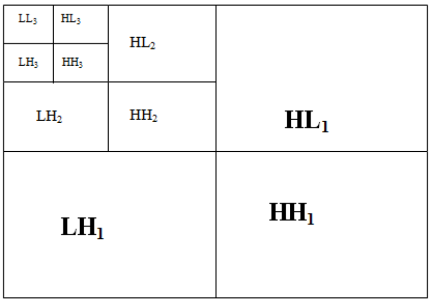


Fig.1 Three Phase Decomposition Using *DWT*

IV. Proposed Work

PSNR, capacity and correlation are major aspects in steganography. More specifically *PSNR* is demanded high, but it depends application to application. *PSNR* is inversely proportional to capacity, and directly proportional to correlation and vice-versa. During the study we found a problem that is of a proper combination of *PSNR*, capacity and correlation is required so that data can be sent through unsecure channel without fear of third party access. The results in the steganography mainly depend on secrete data. The larger value of the secrete data, affect more to the quality of stego image rather than smaller value of secrete data. The database selected for the implementation of proposed approach consists of 3 cover and 9 secrete images in .png format.

4.1 Arnold Transformation

In mathematics, Arnold's cat map is a chaotic map from the torus into itself, named after Vladimir Arnold, who demonstrated its effects in the 1960s. Where x and y are spatial coordinate of a pixel [14].

$$\Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 2.$$

4.2 Data Flow Diagram of the Proposed Approach

In the proposed approach DWT is used for decomposing the image into higher and lower frequency sub bands. Secret data is transformed using Arnold transformation. Data flow diagram of the proposed approach is shown in Fig 2. In proposed approach, the secrete image is divided into *RGB* components and embedded into HL sub band of *RGB* respectively. The same procedure must follow for secrete image #2 and #3.

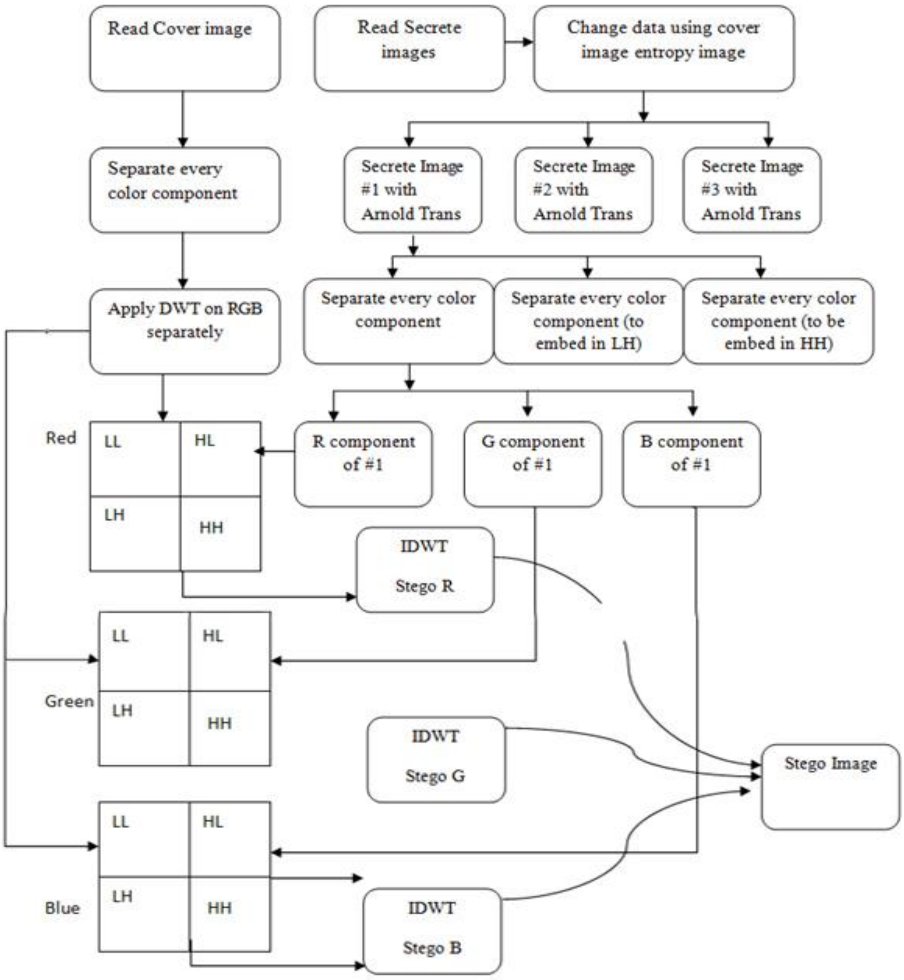

Read Cover image
Read Secrete images
Change data using cover image entropy image
Separate every color component
Secrete Image #1 with Arnold Trans
Secrete Image #2 with Arnold Trans
Secrete Image #3 with Arnold Trans
Apply DWT on RGB separately
Separate every color component
Separate every color component (to embed in LH)
Separate every color component (to be embed in HH)
Red
LL
HL
LH
HH
R component of #1
G component of #1
B component of #1
IDWT
Stego R
Green
IDWT
Stego G
Stego Image
Blue
IDWT
Stego B

Fig. 2 Data Flow Diagram of Proposed Approach

As shown in Fig. 2 read the cover and secrete images and split cover image into its components. Apply DWT on all three components. Change the secrete images using Arnold transform and separate every color component of changed secrete images. Embed the secrete images components into HL, HH, and LH sub band. Apply inverse DWT and obtain stego image.

Recovery procedure is reverse of embedding. Read cover and stego image. Split the cover and stego image into its components. Apply inverse of Arnold transform and get the secrete images.

4.3 Assessment Criteria

From the study it has been found that there are some metrics which can be used to check the performance of particular approach. So the authors considered four metrics for the evaluation of their approach, which are discussed below.

1) *Peak Signal to Noise Ratio (PSNR): The PSNR* depicts the measure of reconstruction of the transformed image. This metric is used for discriminating between the cover and stego image.

$$PSNR = 10 \log 255^2 / MSE$$

2) *Mean Square Error (MSE): MSE* 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 follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - (f'(i,j))^2$$

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 and vice-versa.

3) *Capacity:* Capacity can be formulated as:

$$Capacity = \frac{No.of\ pixels\ of\ secret\ image\ that\ are\ hidden}{No.of\ pixels\ of\ cover\ image\ that\ are\ used\ to\ hide\ data}$$

4) *Correlation:* If we have a series of n measurements of *X* and *Y* written as x_i and y_i where $i = 1,2\ldots n,$ then the sample correlation coefficient can be used to estimate the population Pearson correlation *r* between *X* and *Y*. The sample correlation coefficient is written:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}},$$

Where $\bar{x}$ and $\bar{y}$ are the sample means of *X* and *Y*, and s_x and s_y are the sample standard deviations of X and Y.

V. Experiment

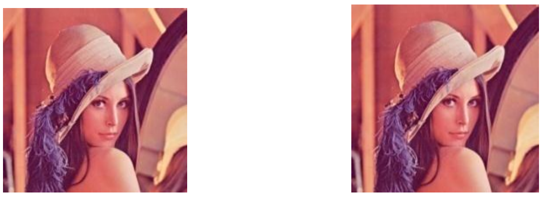
The proposed approach was implemented in MATLAB 7.0 and colored images are used in implementation. Various images used for the experiment are described as under:

Cover Image: In implementation, Lena is used as cover image, of size 512×512. The image is in .png format.

Stego Image: After embedding the data (images) in cover image, stego image obtained. Cover and Stego images are shown below in Fig. 3

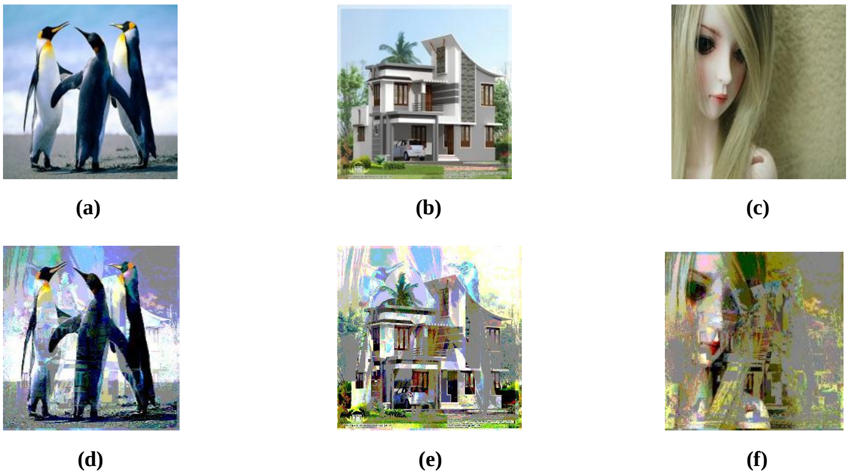
Secrete Image: Nine secrete images of size 256×256(Penguin, House, and Girl) used as data to be hidden in cover image. Each image is in .png format.

Recovered Images: By applying extraction procedure, we recovered secrete images from stego image. All the secret and recovered images are shown in Fig. 4



Cover Image (Lena) **Stego Image (Lena)**

Fig. 3 Cover and Stego Images of Lena



(a) **(b)** **(c)**

(d) **(e)** **(f)**

Fig. 4 Secret Images ((a), (b), (c)) and their Corresponding Recovered Images ((d), (e), (f))

VI. Results

The results of proposed approach are obtained in the form of *PSNR*, Capacity, and Correlation for the images. Execution time of algorithm also calculated.

All the algorithms are implemented in MATLAB 7.0 on a computer of configuration as Pentium(R) Dual CPU 1.73GHz, 1 GB of RAM.

Table 1
PSNRs, Capacity, Correlation and Execution Time as Reported by the Proposed Approach

S. N	Cover Image (png) (512×512)	Secret Image (png) (256×256)	Embedding Factor	*PSNR* (in dB)	*PSNR**1 (in dB)	*PSNR**2 (in dB)	*PSNR**3 (in dB)	Correlation	Capacity (in %)	Execution Time (in Sec.)
1	Lena	Penguins House Girl	0.0075	47.8901	11.6092	11.3043	15.4634	0.9998	75	0.9219
2	Peppers	Baby Hollister Lighthouse	0.0075	48.3925	12.3432	9.8801	14.0006	0.9997	75	0.9375
3	Baboon	Desert Koala Rio	0.0075	47.9144	13.8253	12.3010	10.6291	0.9998	75	0.9063

Table 1 shows the details of cover image and secret images, embedding factor, *PSNR* (cover and stego) and *PSNR** (for all three secret images with their corresponding recovered image), correlation between cover image and stego image, capacity in percentage (pixel embedded in cover divided by cover image's pixels) and real time execution of algorithm.

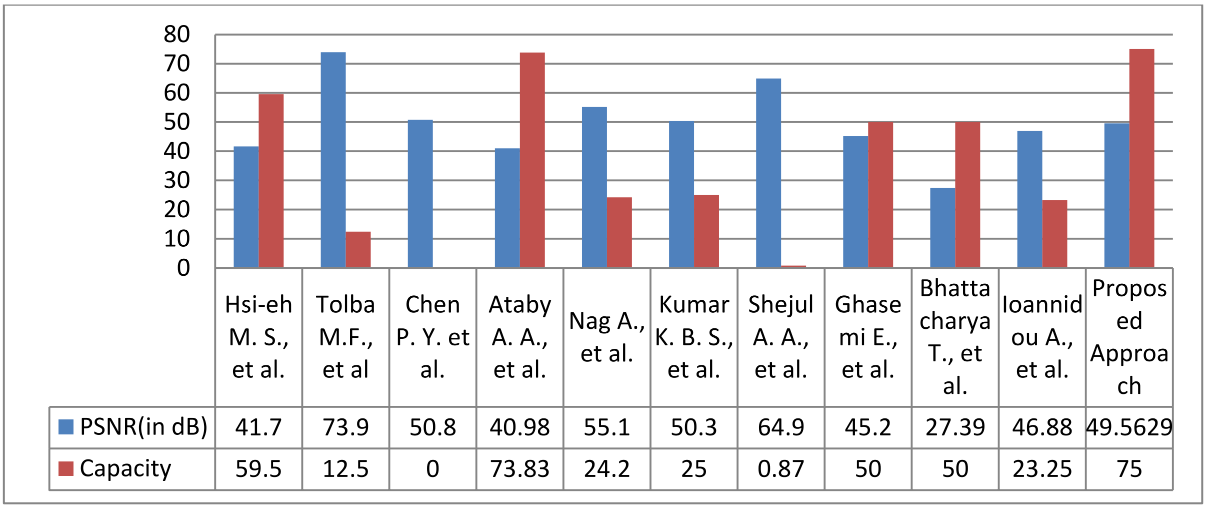
Comparison with Existing Approaches

The proposed approach was compared with existing similar approaches given by authors Hsieh M.S, et al. [3], Tolba M.F, et al. [4], Chen P.Y, et al. [5], Ataby A.A, et al. [6], Nag A., et al. [7], Kumar K.B.S., et al. [8], Shejul A.A., et al. [12], Ghasemi E., et al. [10], Bhattacharya T., et al. [11], Ioannidou A., et al. [13]. The comparison is shown in Table.2.

Table 2
Comparison of Proposed Approach with Similar Existing Approaches

Approach / Metrics	Hsi-eh M. S., et al.	Tolba M.F., et al	Chen P. Y. et al.	Ataby A. A., et al.	Nag A., et al.	Kumar K. B. S., et al.	Shejul A. A., et al.	Ghasemi E., et al.	Bhattacharya T., et al.	Ioannidou A., et al.	Proposed Approach
***PSNR* between cover image and stego image (in dB)**	41.7	73.9	50.8	40.98	55.1	50.30	64.9	45.20	27.39	46.88	**49.5629**

***PSNR* between secrete and recovered (in dB)**	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	**12.0818**
Correlat-ion	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	0.9381	N.A.	**0.9999**
Capacity (in % or bpp)	4.76 *bpp*	1 *bpp*	N.A.	73.83	24.2	25	0.807	50	50	1.89 *bpp*	**75**



	Hsi-eh M. S., et al.	Tolba M.F., et al	Chen P. Y. et al.	Ataby A. A., et al.	Nag A., et al.	Kumar K. B. S., et al.	Shejul A. A., et al.	Ghasemi E., et al.	Bhattacharya T., et al.	Ioannidou A., et al.	Proposed Approach
🟦 PSNR(in dB)	41.7	73.9	50.8	40.98	55.1	50.3	64.9	45.2	27.39	46.88	49.5629
🟥 Capacity	59.5	12.5	0	73.83	24.2	25	0.87	50	50	23.25	75

Fig. 5 *PSNR* and Capacity Comparison among Proposed Approach and Existing Approaches

Fig. 5 shows a graph of comparison among proposed approach and similar existing approaches. It is clear from the graph that, at a particular time *PSNR* value and capacity are contradictory. Both cannot have maximum at same time. In Tolba M.F., et al method *PSNR* is 73.9 dB that is good but capacity is 12.5, which is very less. In Ataby A. A., et al. method capacity is 73 but *PSNR* 22.84 dB, which is again less. Similarly rest approaches have a combination of one parameter good and second not. In this comparison we showed the high capacity with good *PSNR*. The combination of two is good if we talk about rest of approaches. This comparison concludes superiority of the proposed approach.

VII. Conclusion

The work presented in this paper deals with the technique of image steganography using discrete wavelet transform. DWT is applied on color images. Arnold transformation is used to improve security. The proposed approach tries to overcome the demerits of previous similar image steganography approaches.

The results are shown in the form of stego and recovered images. Results of PSNR, capacity and correlation are shown in a table. Analysis of the algorithm is accomplished by comparing the proposed approach with similar existing approaches. From the results, conclusion can be drawn that the proposed approach is superior in terms of PSNR and high embedding capacity.

REFERENCES

[1] A.A. Shejul and U.L. Kulkarni, "A *DWT* based Approach for Steganography Using Biometrics", *IEEE* International Conference on Data Storage and Data Engineering, pp 39-43, 2010.

[2] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Session based Multiple Image Hiding Technique using *DWT* and *DCT*", International Journal of Computer Applications (*IJCA*), Vol. 38, No.5, pp 18-21, 2012.

[3] Ming-Shing Hsieh, Din-Chang Tsebg and Yong-Huai Huang, "Hiding Digital Watermark Using Multiresolution Wavelet Transformation", *IEEE* transactions on industrial electronics, Vol. 48, No. 5, pp 875-882, 2001.

[4] M.F. Tolba, M.A. Ghonemy, I.A. Taha and A. S. Khalifa, "Using Integer Wavelet Transformation in Colored Image-Steganography", *IJICIS*, Vol. 4, No. 4, pp 75-85, 2004.

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

[6] Ali Al-Ataby and 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, pp 358-364, 2010.

[7] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A Novel Technique for Image Steganography Based on *DWT* and Huffman Encoding", International Journal of Computer Science and Security, *(IJCSS*), Vol. 4, No. 6, pp 561-570, 2010.

[8] K B Shiva Kumar, K B Raja and Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", International Journal of Computer Applications (*IJCA*), Vol. 19, No.7, pp 35-40, 2011.

[9] K B Shiva Kumar, Khasim T, K B Raja , Sabyasachi Pattnaik and R. K. Chhotaray, "Dual Transform Technique for Robust Steganography", International Conference on Computational Intelligence and Communication Systems (*ICCICS*), *IEEE* Computer Society, pp 310-314, 2011.

[10] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi, "High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm", International Multiconference of Engineering and Computer Scientist (*IMECS*), Vol. 1, pp. 1-4, 2011.

[11] Tanmay Bhattacharya, Nilanjan Dey and S. R. Bhadra Chaudhuri, "A Novel Session Based Dual Steganographic Technique Using *DWT* and Spread Spectrum", International Journal of Modern Engineering Research (*IJMER*), Vol.1, No. 1, pp-157-161, 2011.

[12] Anjali A. Shejul and Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, February, pp. 16-22, 2011.

[13] Ioannidou A., Halkidis S. T. and Stephanides G., " A Novel Technique for Image Steganography based on a High Payload Method and Edge Detection'', Expert Systems with Applications, Elsevier, Vol. 39, pp. 11517-11524, 2012.

[14] Divya Saxena, "Digital Watermarking Algorithm based on Singular Value Decomposition and Arnold Transform", International Journal of Electronics and Computer Science Engineering(*IJECSE*)", Vol. 1, No. 1, pp 22-27,

[15] Mei-Ching Chen, Sos S. Agaian and C. L. Philip Chen, "Generalized Collage Steganography on Images", IEEE International Conference on Systems, Man and Cybernetics (*SMC*), pp 1043-1047, 2008.

[16] T. Narasimmalou and Allen Joseph. R, "Optimized Discrete Wavelet Transform Based Steganography", *IEEE* International Conference on Advance Communication Control and Computing Technologies (*ICACCCT*), pp 88-91, 2012.