Development and Analysis of Stego Image Using Discrete Wavelet Transform

Umashankar Dewangan[1], Monisha Sharma[2], Swagota Bera[3]

[1]M.E. Scholar (Communication) SSGI, Bhilai, India
umashanker.dewangan@gmail.com

[2]Associate Professor, ECE Department, SSGI, Bhilai, India
monisha.sharma10@gmail.com

[3]Assistant Professor, ECE Department, SSIET, Bhilai, India
swagotab@radiffmail.com

Abstract*: Steganography is an art of hiding one type of information into other information. Steganography exploits the use of a host data to hide a piece of information in such a way that it is imperceptible to a human observer. Wavelet transforms that map integers to integers allow perfect reconstruction of the original image. Hence, we proposed an algorithm that embeds the message bit stream into the LSB's of the discrete wavelet coefficients of a true-color image. The algorithm also applies a preprocessing step on the cover image to adjust saturated pixel components in order to recover the embedded message without lose. It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithms. Experimental results showed the high invisibility of the proposed model even with large message size.*

Keywords: Information hiding, Steganography, Discrete Wavelet Transform (DWT), Inverse Discrete Wavelet Transform (IDWT), Mean Square Error (MSE)

1. Introduction

The development in technology and networking has posed serious threats to obtain secured data communication. This has driven the interest among computer security researchers to overcome the serious threats for secured data transmission. One method of providing more security to data is information hiding. The approach to secured communication is cryptography, which deals with the data encryption at the sender side and data decryption at the receiver side. The main difference between steganography and cryptography is the suspicion factor. The steganography and cryptography implemented together, the amount of security increases. The steganography make the presence of secret data appear invisible to eaves droppers such as key loggers or harmful tracking cookies where the users keystroke is monitored while entering password and personal information. The Steganography is used for secret data transmission. Steganography is derived from the Greek word steganos which means "covered" and graphia which means "writing", therefore Steganography means "covered writing". In steganography the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as carrier to embed the information. The object in which the secret information is hidden is called covert object. Stego image is referred as an image that is obtained by embedding secret image into covert image. The hidden message may be plain text, cipher text or images etc. The steganography method provides embedded data in an imperceptible manner with high payload capacity. Encrypting data provides data confidentiality, authentication, and data integrity. [1]

Steganography, copyright protection for digital media and data embedding are the data hiding techniques. Steganography is a method of hiding secret information using cover images. Copyright marking classified into watermarking and fingerprinting. Watermarking is the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video etc. Fingerprinting attaches a serial number to the copy of digital media. Copyright protection prevents illegal transfer of data. In data embedding systems the receiver will know about the hidden message and the task is to decode the message efficiently. The main aspect of steganography is to achieve high capacity, security and robustness. Steganography is applicable to;

i. Confidential communication and secret data storing

ii. Protection of data alteration

iii. Access control system for digital content distribution,

iv. Media Database systems etc [1].

The various Steganographic techniques are:

i. Substitution technique: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms, etc.

ii. Transform domain technique: The various transform domains techniques are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) are used to hide information in transform coefficients of the cover images that makes much more robust to attacks such as compression, filtering, etc.

iii. Spread spectrum technique: The message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the information. The SNR in every frequency band is small. Hence without destroying the cover image it is very difficult to remove message completely.

iv. Statistical technique: The cover is divided into blocks and the message bits are hidden in each block. The information is encoded by changing various numerical properties of cover image. The cover blocks remain unchanged if message block is zero.

v. Distortion technique: Information is stored by signal distortion. The encoder adds sequence of changes to the cover and the decoder checks for the various differences between the original cover and the distorted cover to recover the secret message [2].

2. Related Work

"Using Integer wavelet transform in colored image steganography", July, 2004 by M.F.Tolba, M.A.Ghonemy and A.Taha [3] proposes an algorithm by which the information capacity can reach 50% of the original cover image. It provides high quality of stego image over the existing LSB based method. "An adaptive steganographic technique based on the integer wavelet transforms", 2009 by R.O.El.Sofy and H.H.Zayed [4] provides high hiding capacity up to 48% of the cover image size. In this paper, we try to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. "A modified high capacity image steganography technique based on wavelet transform", October 2010 by Ali Al-Ataby and Fawzi Al-Naima [5] proposes 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. "A novel approach to develop secure image based steganographic model using Integer wavelet transform" June 2010 by Souvik Bhattacharya, Avinash Prashad and Gautam Sanyal [6] incorporate the idea of secret key for authentication at both the ends in order to achieve high level of security. In this paper, a specific image based steganography technique for communicating information more securely between two locations is proposed. "High capacity and security steganography using discrete wavelet transform", 2010 by H S Manjunatha Reddy and K B Raja [7] propose a high capacity and security steganography using discrete wavelet transform (HCSSD. In this paper the two level wavelet transform is applied as cover and payload. The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta.

"A Steganographic method based on Integer wavelet transform & Genetic Algorithm", 2011 by Elham Ghasemi, Jamshid and Brahram [8] propose a novel steganography scheme based on Integer Wavelet Transform and Genetic Algorithm. Simulation results show that the novel scheme outperforms adaptive steganography technique based on integer wavelet transform in term of peak signal to noise ratio and capacity, 35.17 dB and 50% respectively. "Digital steganography implementation for colored images using wavelets", July 2011 by T.C.Manjunatha and Usha Eswaran [9] uses embedding process stores upto 4 message bits in each integer co-efficient for all the transform sub-bands. This paper presents a conceptual view of the digital steganography & exploits the use of a host data to hide a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but easily detected by a computer. "A novel technique for image steganography based on DWT and Huffman encoding", 2011 Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar [10] presents a technique for image steganography based on DWT. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. First, two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band.

"Efficient capacity image steganography by using Wavelets", 2011 by Yedla Dinesh and Addanki Purna Ramesh [11] perform a multi-resolution analysis and space frequency localization. As compared to the current transform domain data hiding methods this scheme can provide an efficient capacity for data hiding without sacrificing the original image quality. "Improved image steganography technique for colored images using Wavelet transform", February 2012 by Saddaf Rubab and M.Younus [12] derives a new algorithm to hide our text in any colored image of any size using wavelet transform. It improves the image quality and imperceptibility. Their method sustains the security attacks. This new method gives better invisibility and security of communication. This method provides double security by involving blowfish, which satisfies the need of imperceptibility. "Edge adaptive image steganography in DWT domain", February 2012 by S.Priya and A.Amsaveni[13] gives LSB based edge adaptive image steganography. Edge adaptive stenography on frequency domain improves security and image quality compared to the edge adaptive stenography on spatial domain. "Steganography based on DWT transform", February 2012 Rastislav Hovancak, Peter Foris and Dusan Levicky [14] propose a new method of steganography technique based on DWT transform. The proposed method has ability to hide secret message in a digital image. The secret message is embedded into the image by changing wavelet co-efficient. The quality of the stego image is of the proposed method is very close to that of the original one.

3. Model

The definitions, Wavelet Transform and proposed model are described in this section.

Definitions:

• **Cover Image**: It is defined as the original image into which the required secret message is embedded. It is also termed as innocent image or host image. The secret message should be embedded in such a manner that there are no significant changes in the statistical properties of the cover image. Good cover images range from gray scale image to colored image in uncompressed format.

• **Payload**: It is the secret massage that has to be embedded within the cover image in a given Steganographic model. The payload can be in the form of text, audio, images, and video.

• **Stego image**: It is the final image obtained after embedded the payload into a given cover image. It should have similar statistical properties to that of the cover image.

• **Hiding Capacity**: The size of information that can be hidden relative to the size of the cover without deteriorating the quality of the cover image.

• **Robustness**: The ability of the embedded data to remain intact if the stego image undergoes transformation due to intelligent stego attacks.

• **Security**: This refers to eavesdropper's inability to detect the hidden information.

• **Mean Square Error (MSE)**: It is the measure used to quantify the difference between the initial and the distorted or noisy image. Let Pi represents the pixel of one image of size N and Qi that of the other

$$MSE = \sum_{i=1}^{all\ pixels} \sum_{i=1}^{all\ pixels} \frac{(Cover(i,j) - Stego(i,j))2}{N \times N}$$

From MSE we can find Peak Signal to Noise Ratio (PSNR) to access the quality of the Stego image with respect to cover image given by

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}$$

Wavelet Transform: It converts an image from time or spatial domain to frequency domain. It provides a time frequency representation. The Wavelet Transform is obtained by repeated filtering of the coefficients of the image row-by-row and column-by-column.

- **Approximation Band**: It is the band having the lower frequency coefficients of the image in the wavelet domain. It contains all the significant features of the image.

- **Inverse Wavelet Transform**: It is applied over the stego image to convert it from frequency domain to spatial domain. Hence it is frequency-time representation.

Wavelet transform is used to convert a spatial domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients.

The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image.

4. Algorithm

4.1 Data Embedding Algorithm

The proposed approach for data hiding comprises of the following steps:

1) Get the Cover Image and Secret message.
2) Calculate the length of the secret message.
3) Perform the Discrete Wavelet Transform of the cover image with haar wavelet.
4) Select any of the wavelet coefficients (redundant coefficients) from the obtained high frequency coefficients.
5) Select any one of the pixels from red, green and blue.
6) Now the selected coefficients are processed to make it fit for modification or insertion.
7) The secret message plus the message length is embedded into this processed coefficients.
8) This modified coefficient is now merged with the unmodified coefficients.
9) Finally, the inverse DWT (IDWT) is applied to obtain the Stego image.
10) Stego image will be obtained.

4.2 Data Extraction Algorithm

The proposed approach for data extracting comprises of the following steps:

1) Get the Stego Image.
2) Perform the Discrete Wavelet Transform of the stego image with haar wavelet.
3) Select the same sub-band from the obtained coefficients.
4) Select the desired pixels to process it.

4) Process the selected pixel's coefficients to make it fit for extraction.
5) Now extract the message length and the secret message from these processed coefficients.
6) This gives us the Secret message

5. Results And Performance Analysis

For performance analysis we considered the Cover Images (CI) such as Koala, Tulip, Penguin, Desert & Chrysanthemum Image. Payload images (PL) are Penguin, Koala, Tulip, Chrysanthemum and Desert. The payload is embedded into the cover image to derive the Stego image at the sending end. The payload is recovered from the Stego image at the destination with minimum distortion. Fig. 1(a), 2(a), 3(a), 4(a) and 5(a) are the Cover Images (CI). Fig. 1(b), 2(b), 3(b), 4(b) and 5(b) are the Payload images (PL). Fig. 1(c), 2(c), 3(c), 4(c) and 5(c) are the Stego Images (SI). Fig. 1(d), 2(d), 3(d), 4(d) and 5(d) are the Retrieved Payload images (RPL). Table I shows the experimental results of the proposed algorithm with respect to Embedding capacity and Execution Time. Table II shows the experimental results of the proposed algorithm with respect to MSE and PSNR between the cover image and Stego image. The PSNR, MSE, embedding capacity & execution time are dependent on image formats and sizes of the cover and Stego image.

Table I: Comparison between different images with respect to embedding capacity & execution time

Image	*Embedding Capacity*	*Execution Time*
India Gate & HP	45KB	5.0225 Sec.
Sunset & WWF	34KB	3.4563 Sec
Dolphin & Intel	29KB	4.2319 Sec
Tiger & Android	41KB	4.6529 Sec.
Mothers Day & NASA	33KB	5.5462 Sec.

Table II: Comparison between different images with respect to MSE & PSNR

Image	*MSE*	*PSNR (dB)*
India Gate & HP	0.0081685	69.0094
Sunset & WWF	0.008478	68.8445
Dolphin & Intel	0.0084059	68.8814
Tiger & Android	0.0052215	70.9529
Mothers Day & NASA	0.0083025	68.9387

Fig. 1 (a)

Fig. 1 (b)

Fig. 1 (c)

Fig. 1 (d)

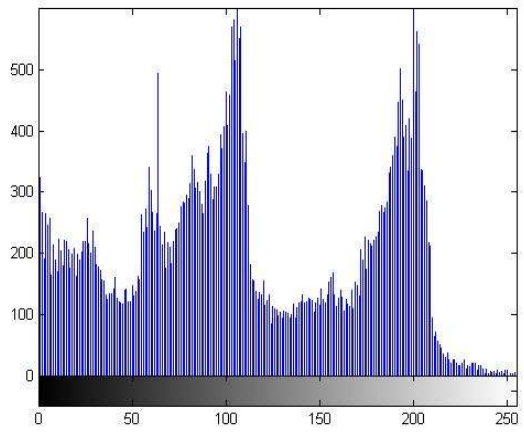

Fig. 1 (e) : Histogram of Cover Image

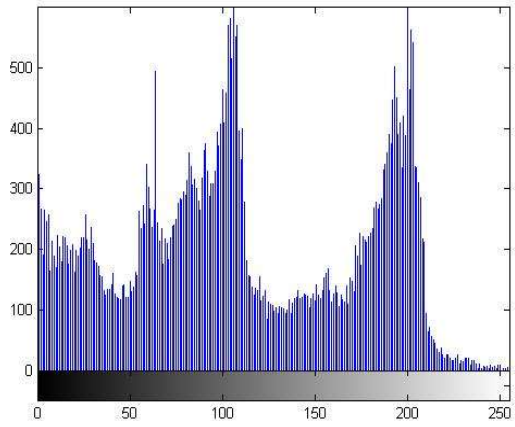

Fig. 1 (f) : Histogram of Stego Image

Fig. 1 : India Gate & HP Image

Fig. 2 (a)

Fig. 2 (b)

Fig. 2 (c)

Fig. 2 (d)

Fig. 3 (c)

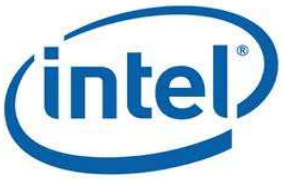

Fig. 3 (d)

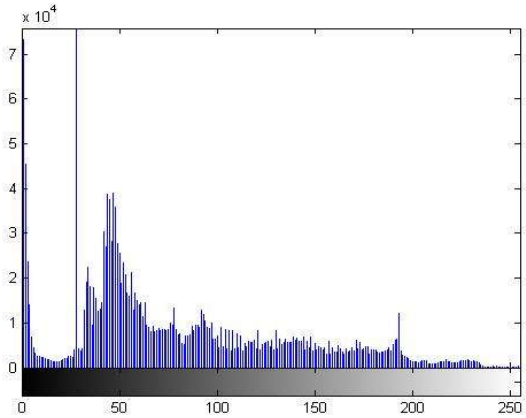

Fig. 2 (e) : Histogram of Cover Image

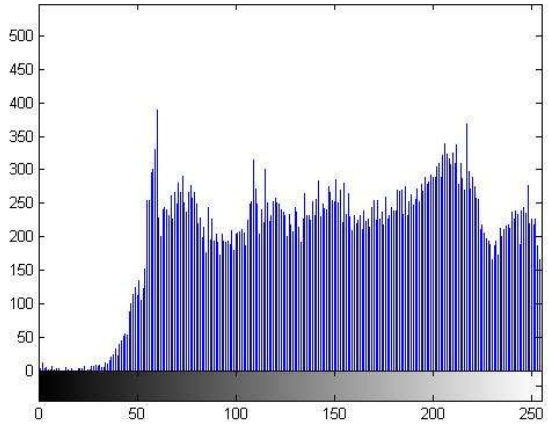

Fig. 3 (e) : Histogram of Cover Image

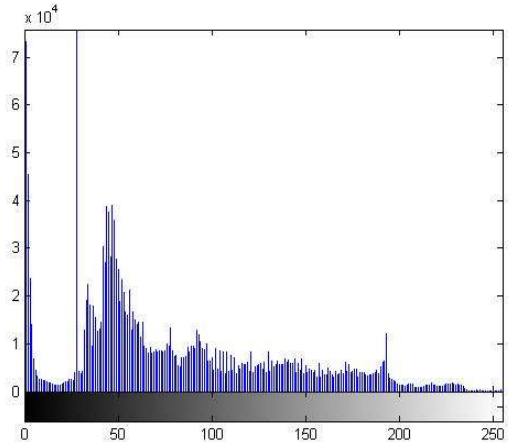

Fig. 2 (f) : Histogram of Stego Image

Fig. 2 : Sunset & WWF Image

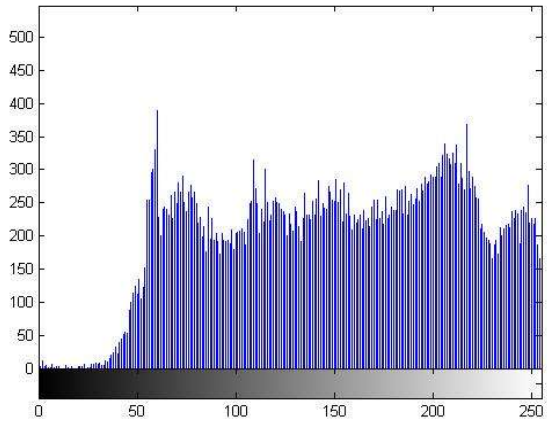

Fig. 3 (f) : Histogram of Stego Image

Fig. 3 : Dolphin & Intel Image

Fig. 3 (a)

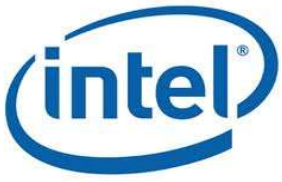

Fig. 3 (b)

Fig. 4 (a)

Fig. 4 (b)

Fig. 4 (c)

Fig. 4 (d)

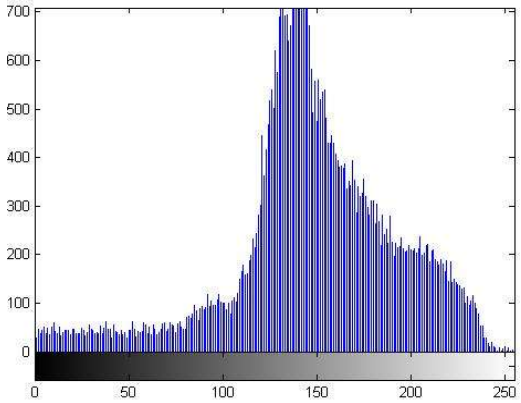

Fig. 4 (e) : Histogram of Cover Image

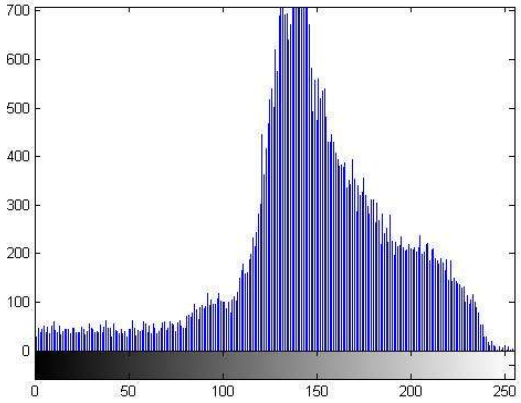

Fig. 4 (f) : Histogram of Stego Image

Fig. 4 : Tiger & Android Image

Fig. 5 (c)

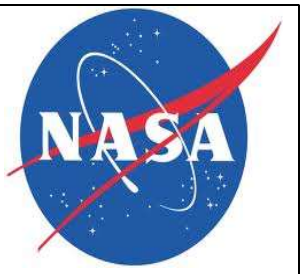

Fig. 5 (d)

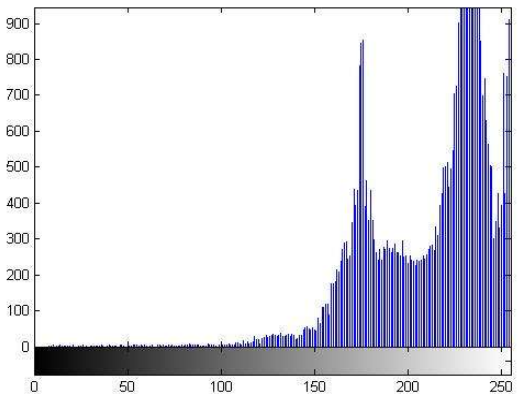

Fig. 5 (e) : Histogram of Cover Image

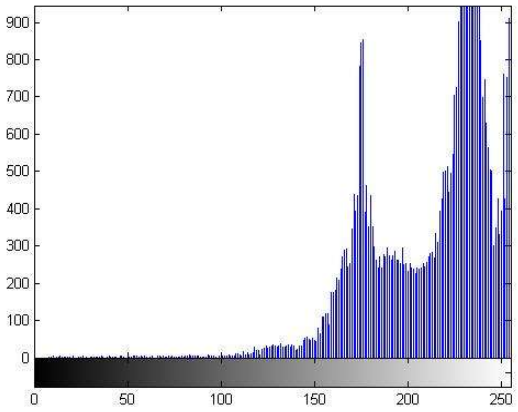

Fig. 5 (f) : Histogram of Stego Image

Fig. 5 : Mothers Day & NASA Image

Fig. 5 (a)

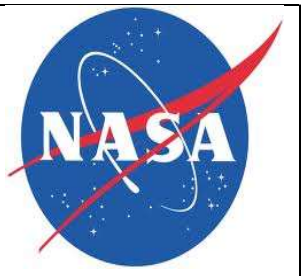

Fig. 5 (b)

6. Conclusions

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We pointed out the enhancement of the image Steganographic system using DWT approach to provide a means of secure communication. In our proposed approach, the message bits are embedded randomly into the cover-image pixels instead of sequentially. After testing the system and studied the recorded results from the experiment. Generally, image steganography method does not provide much attention on the basic demand of secrecy and privacy. In this project, the major importance is given on the secrecy as well as the privacy of information. The embedding process is hidden under the transformation (DWT and IDWT) of cover image. These operations provide sufficient secrecy. After comparing with previous existing algorithms, it is found that we get highest PSNR then the existing one.

We have achieved our aim of both improving Steganographic capacity and imperceptibility. We have achieved a PSNR value up to 80 dB, which is our major advantage. Here lies the novelty of our research work.

[1] Neil F. Johnson and Sushil Jajodia, "Steganalysis: The Investigation of Hidden Information," IEEE conference on Information Technology, pp. 113-116, 1998.

[2] Lisa M.Marvel and Charles T. Retter, "A Methodlogy for Data Hiding using Images," IEEE conference on Military communication, vol. 3, Issue. 18-21, pp. 1044-1047, 1998.

[3] "Using Integer Wavelet Transforms in Colored Image Steganography", M. F. Tolba, M.A. Ghonemy, I. A. Taha, and A. S. Khalifa, IJICIS Vol. 4 No. 2, July 2004.

[4] "An adaptive Steganographic technique based on the integer wavelet transforms", R.O.El.Sofy, H.H.Zayed, 978-1-4244-3778-8/09/$25.00 ©2009 IEEE

[5] "High capacity and security steganography using discrete wavelet transform", H S Manjunatha Reddy, K B Raja, Dept. of Electronics and Communication, Global Academy of Technology, Bangalore, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).

[6] "A Novel approach to develop secure image based Steganographic model using Integer wavelet transform" Souvik Bhattacharya, Avinash Prashad, Gautham Sanyal, 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[7] "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" Ali Al- Ataby, and Fawzi Al-Naima, The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.

[8] "A Steganographic method based on Integer Wavelet Transform & Genetic Algorithm" Elhan Ghasemi, Jamshid & Brahram, Islamic Azad University Science and Research Branch, 978-1-4244-9799- 7/111$26.00 ©20 11 IEEE.

[9] "Digital Steganography Implementation for colored Images using Wavelet" T.C. Manjunath, Usha Eswaran, International Journal of Communication Engineering Applications-IJCEA- Vol 02, Issue 04; July 2011, ISSN: 2230-8520; e-ISSN-2230-8539

[10] "A novel technique for image steganography based on DWT and Huffman encoding", Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2,2011.

[11] Efficient Capacity Image Steganography by Using Wavelets Yedla dinesh Addanki purna ramesh (Department of Electronics and communications, Sri vasavi engineering college, Tadepalligudem, AP, India) (Department of Electronics and communications, Sri vasavi engineering college, Tadepalligudem, AP, India).

[12] Improved Image Steganography Technique for Colored Images using Wavelet Transform Saddaf Rubab department of Computer Engineering, College of Electrical & Mechanical Engineering, National University of Sciences & Technology (NUST), Islamabad, Pakistan M. Younus Department of Computer Engineering, College of Electrical & Mechanical Engineering, National University of Sciences & Technology (NUST), Islamabad, Pakistan.

[13] Edge Adaptive Image Steganography in DWT Domain, S. Priya and A. Amsaveni,Bonfring International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2,February 2012.

[14] Steganography based on dwt transform Rastislav Hovančák, Peter Foriš, Dušan Levický Department of Electronics and Multimedia Telecommunications, Technical University of Košice, Park Komenského 13, 041 20 Košice, Slovak Republic.

Author profile

Umashankar Dewangan received his B.E. degree in Electronics & Telecomm, from SSCET, Bhilai (C.G.) in 2009. Currently he is doing ME in Communication from the same college. The above algorithm is designed by him under the guidance of his project guide Dr. (Mrs.) Monisha Sharma & Mrs. Swagota Bera.