IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48
www.iosrjournals.org

A Review of Comparison Techniques of Image Steganography

[1]Stuti Goel,[2]Arun Rana,[3]Manpreet Kaur

Abstract: *Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image viz., text, video, and image (payload) without causing statistically significant modification to the cover image. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected.This paper deals with hiding text in an image file using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based steganography.The LSB algorithm is implemented in spatial domain in which the payload bits are embedded into the least significant bits of cover image to derive the stego-image whereas DCT & DWT algorithm are implemented in frequency domain in which the stego-image is transformed from spatial domain to the frequency domain and the payload bits are embedded into the frequency components of the cover image.The performance and comparison of these three techniques is evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness.*

Keywords: *Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Steganography, MSE, PSNR*

I. Introduction

Therapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography[1].In the present year, secure and hidden communication is the foremost requirement of the people. Therefore steganography is gaining attraction by people due to the security issues over internet. Steganography means covert writing. Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file[8]. The objective of steganography is hiding the payload (embedded information) into the cover image such that the existence of payload in the cover image is imperceptible to the human beings[14]. There are different techniques to implement steganography namely least significant bit (LSB),discrete cosine transform (DCT) & discrete wavelet transform(DWT) technique.

There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain[6]. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then processing is applied on the transformed coefficients.

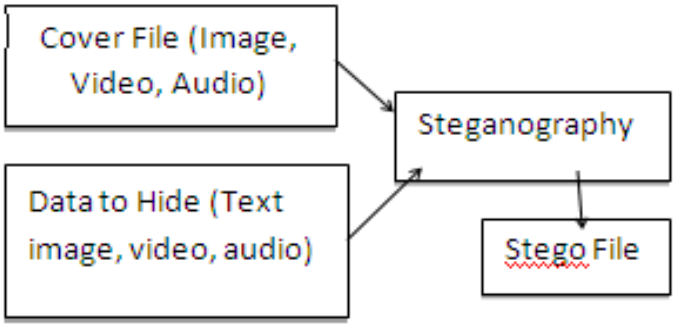

Fig1: The process of hiding data[8]

LSB technique is implemented in spatial domain while DCT & DWT technique are implemented in frequency domain. In least significant bit(LSB), each pixel of an image transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc. The discrete cosine transforms (DCT)& discrete wavelet transform (DWT) are mathematical function that transforms digital image data from the spatial to the frequency domain.In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for lossy compression while In DWT, secret

messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness.

II. Literature Survey

J.R.Krenn explained steganography and its implementation techniques [1]. Deshpande Neeta, et. al. proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This paper explains the LSB embedding technique and presents the evaluation results for 2, 4, 6 Least significant bits for a .png file and a .bmp file[2].K.B.Raja, et. al.proposed a challenging task of transferring the embedded information to the destination without being detected. In this paper, the image based steganography that combines Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and compression techniques on raw images to enhance the security of the payload[3]. Vijay Kumar Sharma,et. al. has worked upon a new steganography algorithm for 8bit (gray scale) or 24bit (color image) based on Logical operation to ensure the security against the steganalysis attack[4]. Po-YuehChen,et. al. proposed a new steganography technique which embeds the secret messages in frequency domain. According to different users' demands on the embedding capacity and image quality, the proposed algorithm is divided into two modes and 5 cases[5]. Chen Ming,et. al.focused on the steganography tools algorithms. Based on the analyses of the algorithms, various tools are divided into five categories: (1). Spatial domain based steganography tools; (2). Transform domain based steganography tools; (3). Document based steganography tools; (4) File structure based Steganography tools; (5)other categories, e.g. video compress encoding and spread spectrum technique based [6]. Aneesh Jain,et. al.proposed a scheme which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and this new image and which is also resistant to JPEG compression[7].BeenishMehboob,et. al. discusses the art and science of Steganography in general and proposes a novel technique to hide data in a colorful image using least significant bit[8]. Hassan Mathkour,et. al. seta a criteria to analyze and evaluate the strengths and weaknesses of the presented techniques and a more robust steganography technique has been developed that takes advantages of the strengths and avoids the limitations[9]. NageswaraRaoThota,et. al.attempted to implement basic JPEG compression using only basic MATLAB functions[10].MamtaJuneja, et. al. discusses the design of a Robust image steganography technique based on LSB (Least Significant Bit) insertion and RSA encryption technique[11]. K.B.Shiva Kumar, et. al. discusses the important issue of modern communication is establishing secret communication while using public channel and is achieved by steganography. In this paper, Coherent Steganography Technique using Segmentation and Discrete Cosine Transform (CSSDCT) is proposed. The cover image is divided into 8*8 blocks and DCT is applied on each block. The number of payload MSB bits is embedded into DCT coefficients of the cover image coherently based on the values of DCT coefficients. It is observed that the proposed algorithm has better PSNR, Security and capacity compared to the existing techniques[12]. Dr. EktaWalia, et. al. presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography [13]. K Suresh Babu, et. al.proposed an image Steganography that can verify the reliability of the information being transmitted to the receiver. The method can verify whether the attacker has tried to edit, delete or forge the secret information in the stego-image[14].Atalla I. Hashad,et. al. describe the LSB insertion technique, the Discrete Cosine Transform (DCT) insertion technique is described and finally we will propose a new technique that uses the idea of inserting a bit in the spatial domain combined with the DCT insertion technique[15]. ArvindKumar, et. al.discusses how digital images can be used as a carrier to hide Messages and also analyses the performance of some of the steganography tools[16]. Vijay Kumar, et. al.intends to observe the effect of embedding the secret message in different bands such as CH, CV and CD on the performance of stego image in terms of Peak Signal to Noise Ratio (PSNR). Experimentation has been done using six different attacks. Experimental results reveal that the error block replacement with diagonal detail coefficients (CD) gives better PSNR than doing so with other coefficients[17]. Ali Al-Ataby, et. al .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[18]. T. Narasimmalou, et. al.Proposed an optimal discrete wavelet transform (DWT) based steganography.Experiments show that the peak signal noise ratio (PSNR) generated by the proposed method is better[19]. NedaRaftari,et. al. proposed a novel image steganography technique that combines the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) is proposed which embeds secret image in frequency domain of cover image with high matching quality[20].

III. Methods Of Concealing Datain Digital Image

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image. In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

3.1 Least significant bit substitution Technique(LSB):

In LSB steganography, the least significantbits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values[4]:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

1101001**1**
0100101**0**
1001011**0**
1000110**0**
0001010**0**
0101011**0**
0010011**1**
0100001**1**

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye.

However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB. LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format [8].

Another example of LSB technique is:Consider a grid for 3 pixels of a 24-bit image and the number 300 is to be embedded using LSB technique. The resulting grid is as follows:

PIXELS: (01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 10110010 10110101)

C: 10000011

(0101010**1** 0101110**0** 1101100**0)**
(1011011**0** 1111110**0** 0011010**0)**
(1101111**1**10110011 1011010**1)**

Here the number C was embedded into the first 8 bytes of the grid, only the 2 bits needed to be changed according to the embedded message .On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

3.2 Discrete Cosine Transform Technique(DCT):

DCT coefficients are used for JPEG compression[10][12]. It separates the image into parts of differing importance. 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.

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 [13]. 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. The general equation for a 1D (N data items) DCT is defined by the following equation:[12]

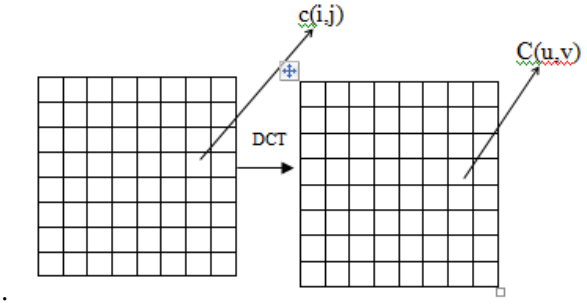

Fig2:Discrete Cosine Transform of an Image[12]

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

Where u= 0, 1, 2….. N-1

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:[12]

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

Where u, v = 0,1,2….N-1

Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix.
DCT is used in steganography as[10]-
Image is broken into 8×8 blocks of pixels.
Working from left to right, top to bottom,
DCT is applied to each block.
Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

3.3 Discrete Wavelet Transform Technique (DWT)[5]:

The frequency domain transform we appliedin this research is Haar-DWT, the simplestDWT[18][19]. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other is the vertical one.Detailed procedures of a 2-D Haar-DWT aredescribed as follows:
Step 1: At first, scan the pixels from left toright in horizontal direction. Then, performthe addition and subtraction operations onneighboring pixels. Store the sum on the leftand the difference on the right as illustrated in Figure 3. 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 high frequency part of the original image (denoted as symbol H).

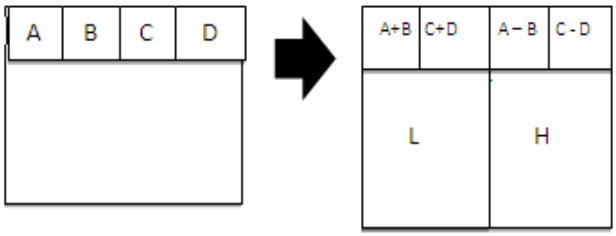

Fig 3: The horizontal operation on first row[5]

Step 2: Secondly, scan the pixels from top tobottom 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 Figure 4. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.

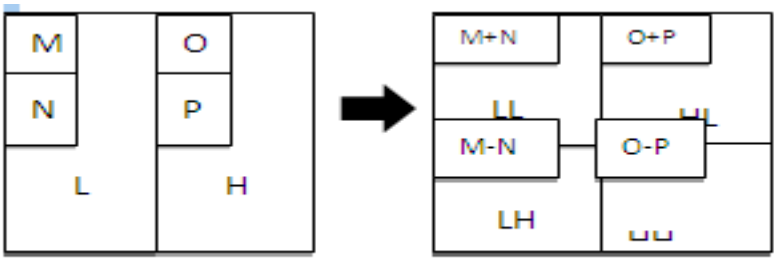

Fig.4 The vertical operation[5]

IV. Algorithm of steganography

4.1 LSB Based Steganography:[12]

Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

4.2 DCT Based Steganography:[12]

Algorithm to embed text message:-

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

4.3 DWT Based Steganography:

Algorithm to retrieve text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D-Haar transform on the cover image.
Step 3: Obtain the horizontal and vertical filtering coefficients of the cover image. Cover image is added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Obtain the horizontal and vertical filtering coefficients of the cover image. Extract the message bit by bit and recomposing the cover image.
Step 4: Convert the data into message vector. Compare it with original message.

V. Evaluation of Image Quality:

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.

5.1 Mean-Squared Error:

The mean-squared error (MSE) between two images I1(m, n) and I2 (m, n) is[2]:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

M and *N* are the number of rows and columns in the input images, respectively.

5.2 Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range[5]:

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

5.3 Capacity:

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganography embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Therefore capacity depends on total number of bits per pixel & number of bits embedded in each pixel. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage[13].

5.4 Domain Type (DOM):

DOM is either Spatial(S) or Transform (T). The techniques that use transform domain hide information in significant areas of the cover images and may be more complex for attackers[9].

VI. Result & Conclusion

Comparative analysis of LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR , MSE , Robustness&Capacity on different images and the results are evaluated.If PSNR ratio is high then images are best of quality.

6.1 LSB Substitution Technique:


(a) Jet

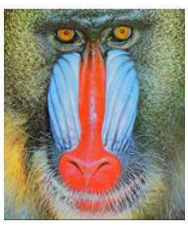
(b) Baboon

Table 6.1 LSB substitution technique[21]:

Cover image	PSNR(dB)	MSE(dB)
Jet	52.7869	.58505
Baboon	53.7558	.52329

6.2 DCT Transform Technique:


(a) Jet


(b) Baboon

Table 6.2 DCT transform technique[22]:

Cover image	**PSNR(dB)**	**MSE(dB)**
Jet	55.6473	.420896
Baboon	58.3766	.30740

6.3 DWT Transform Technique:


(a) Jet

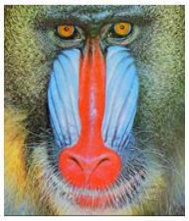
(b) Baboon

Table 6.3 DWT transform technique[23]:

Cover image	**PSNR(dB)**	**MSE(dB)**
Jet	44.76	1.4741
Baboon	44.96	1.4405

Table 6.4 Parameters analysis of steganography Methods: [24]

Features	**LSB**	**DCT**	**DWT**
Invisibility	Low	High	High
Payload capacity	High	Medium	Low
Robustness against image manipulation	Low	Medium	High
PSNR	Medium	High	Low
MSE	Medium	Low	High

VII. Conclusion

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. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself [24].In this paper, analysis of LSB, DCT & DWT methods has been successfully implemented and results are delivered. The MSE and PSNR of themethods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. The PSNR shows the quality of image after hiding the data. From the results, it is clear that PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image. An embedding algorithm is said to be ROBUST if the embedded message can be extracted after the image has been manipulated without being destroyed. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

References

[1] J.R. Krenn, "Steganography and Steganalysis", January 2004.

[2] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[3] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE-0-7803-9588-3/05/$20.00 ©2005.

[4] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minizedetection."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.

[5] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography",International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.

[6] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, "Analysis of Current Steganography Tools: Classifications & Features" , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06),IEEE- 0-7695-2745-0/06 $20.00 © 2006.

[7] AneeshJain,IndranilSen.Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07/$25.00©2007.

[8] BeenishMehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427-6/08/$20.00 ©2008.

[9] Hassan Mathkour, Batool Al-Sadoon, AmeurTouir, "A New Image Steganography Technique",IEEE-978-1-4244-2108-4/08/$25.00 © 2008.

[10] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[11] MamtaJuneja,Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[12] Dr. EktaWalia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography" ,Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[13] K.B.ShivaKumar,K.B.Raja, R.K.Chhotaray, SabyasachiPattnaik, "Coherent Steganography using Segmentation and DCT",IEEE-978-1-4244-5967-4/10/$26.00 ©2010.

[14] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication of Secret Information in Image Steganography" .

[15] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010.

[16] Atalla I. Hashad,Ahmed S. Madani, "A Robust Steganography Technique Using Discrete Cosine Transform Insertion" .

[17] Vijay Kumar, Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography" ,IEEE- 978-1-4244-4791-6/10/$25.00_c 2010.

[18] 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, October 2010.

[19] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.

[20] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.

[21] AnkitaSancheti, "Pixel Value Differencing Image Steganography Using Secret Key" International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-1, and December 2012.

[22] NehaBatra&PoojaKaushik, "Implementation of Modified 16×16 Quantization Table Steganography on Color Images", International Journal of Advanced Research in Computer Science and Software Engineering,ISSN: 2277 128X, Volume 2, Issue 10, October 2012.

[23] ElhamGhasemi, JamshidShanbehzadeh, NimaFassihi, "High Capacity Image Steganographyusing Wavelet Transform and Genetic Algorithm", proceedings of international multiconfrence of engineers & computer science, IMECS-Volume I,March 16-18,2011

[24] GurmeetKaurandAartiKochhar, "A Steganography Implementation based on LSB & DCT", "International Journal for Science and Emerging, Technologies with Latest Trends" 4(1), ISSN No. (Online):2250-3641, ISSN No. (Print): 2277-8136, 35-41 (2012)