ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Data Hiding in Color Images Using Modified Quantization Table

Neha Batra[1] Pooja Kaushik[2]

[1] Pursuing M.Tech, Dept., of ECE, MMU, Mullana, India
[2]Assistant Professor, Dept., of ECE, MMU, Mullana, India

Abstract— ***With the rapid growth of of internet and wireless networks, information security becomes significant to protect e-commerce and personal privacy. Data Hiding is an important issue for information security.There has been number of steganographic embedding techniques proposed over last few years. This paper presents a novel steganographic method based on the JPEG quantization table modification. Instead of dividing cover image into 8×8 blocks, the cover image is divided into nonoverlapping blocks of 16×16 pixels to embed secret information. Here we have considered color images and investigated the feasibility of data hiding. Four performance parameters namely Capacity, MSE and PSNR and NC have been compared on different sizes of standard test images. In comparison with Jpeg-Jsteg and Chang et al. methods based on the conventional blocks of 8x8 pixels the proposed method shows high performance with regard to embedding rate and PSNR of stego image. Furthermore, NC shows that the produced stego-images are almost similar to the original cover images.***

Index Terms — Capacity, DCT, JPEG, PSNR, Steganography

I. INTRODUCTION

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" [5] defining it as "covered writing". In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [16]. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography is often confused with Cryptography because the two are similar in the way that they both are used to protect important information. The difference between the two is that, Cryptography scrambles the message so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper's attention. Steganography hides the secret message within other innocuous-looking cover files (i.e. images, music and video files) so that it cannot be observed.

Three different aspects in information-hiding systems contend with each other, these are capacity, security, and robustness[4].Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information. Information hiding generally relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness—that is, it should be impossible to remove a watermark without degrading the data object's quality.

Data hiding methods for images can be categorized into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain [12, 13], the secret messages are embedded in the image pixels directly. In the frequency-domain [13, 14], however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed coefficients. In recent years, digital JPEG images have become the most popular images on the internet, primarily because they take less space than other images and provide great visual quality with typical compression methods. Therefore, steganography techniques based on digital JPEG images have been greatly developed.
It applies the discrete cosine transformer (DCT) to image which is a widely used tool for frequency transformation. There is a JPEG hiding-tool called Jpeg–Jsteg [8]. The main drawback of Jpeg–Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coefficients are almost all zero and cannot hide messages. Both color and gray scale images can be used as cover images because some steganography methods use color JPEG images as test images while others use gray scale images [9].
The paper is organised in the following sections:
Section II reviews the related work on JPEG steganographic methods. Section III describes our proposed steganographic model and discusses the algorithms used for embedding and

abstracting process. Performance analysis and attributes of our proposed method are discussed in section IV. Finally the conclusion is presented in section V.

II. RELATED WORK

Steganography based on JPEG applies 2-D DCT transform. The process starts by dividing the cover image into blocks of 8x8 pixels, performing DCT and finally using standard 8x8 quantization tables, a well-known steganographic tool is Jsteg, which embeds secret data in LSB. Since it inserts only 1 bit in each quantized coefficient whose value is not -1,0,+1, this makes the capacity very limited [1,3-4,12]. Huang et al [2] proved the feasibility of embedding information in quantized DC coefficient through experiments. By using embedding of middle frequency coefficients, Chang et al [6], Tseng et al [7] and Yu et al [10] proposed a high capacity steganography with modified 8x8 quantization tables.

Based on Chang's quantization paper Jiang Cuiling et al [17] proposed a method of dividing the cover image into 16×16 pixels which resulted in better quality stego images and higher capacity on gray scale images.Increasing the capacity of cover images while maintaining imperceptibility is still a challenge on color images. Since the significant DCT coefficients of 16x16-pixels blocks are limited, more middle frequency coefficients can be used for embedding. This might increase the embedding capacity and preserve image quality. We suggest a steganographic method based upon blocks of 16x16 pixels and modified 16x16 quantization table. Therefore, we are going to use the same technique used by Chang et al. However, we divide the cover image into non-overlapping blocks of 16x16 pixels and use larger quantization table in order to improve the embedding capacity in color images.

III. PROPOSED WORK

In this section evaluation parameters, proposed embedding and retrieval techniques are discussed:

A. Evaluation Parameters

Most researchers use Peak Signal to noise ratio (PSNR), Mean Square Error (MSE) and Hiding Capacity as performance parameters to measure the quality of image.

(a) MSE: It is defined as square of error between cover & stego image. The error indicates the distortion in an image.

MSE can be calculated by using 2-D mathematically equation described as follows:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M} \sum_{j=1}^{N} \left(X_{ij} - \bar{X}_{ij}\right)^2$$

Where X_{ij} = The value of pixel in cover image

$\bar{X}_{ij}$ = The value of pixel in stego image

N=Size of image

(b) PSNR: It is measure of quality of image.

PSNR can be calculated by using mathematically equation given below:

$$PSNR = 10 \times \log \frac{255^2}{MSE} \text{db}$$

(c) NC: It determines the similarity between cover image and stego image. Equation for NC is given below:

$$NC = \left(\frac{\sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij} * \bar{X}_{ij}}{\sum_{i=1}^{M} \sum_{j=1}^{N} X_{ij} * X_{ij}} \right)$$

(d) CAPACITY

Steganographic capacity is the maximum no of bits that can be embedded in a cover image with a negligible probability of detection by an adversary. Namer.N.EL-Emam et al [11] defines the capacity as the size of the hidden message relative to the size of stego image. It is represented by bits per pixel (bpp) and in terms of percentage it is given as MHC.

B. Proposed 16×16 Quantized Table Embedding Technique for Color Images.

Inspired by the design of quantization table [11, 13-15] a new quantization table approach is proposed whose length is twice the standard quantization table. The process results in both DC & AC coefficients of low & mid frequency parts. So there are 136 AC coefficients in quantization table which are set to 1 that can embed secret information. As a result stego capacity is enhanced. For comparison if we consider test image of 512×512 as an example, chang's method has 26 coefficients, where each coefficient can embed two bits. So total embedment done is 2×26×512×512/8×8 = 212992 bits. With proposed method, Capacity is 2×136×512×512/16×16 = 278528 bits.

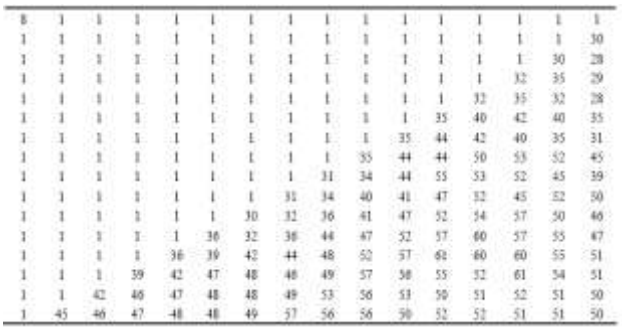

Figure 1: 16×16 Modified Quantization Table

ALGORITHMS

The embedding procedure contains five phases. They are Color image Pre-processing, Message Encryption, Message embedment, Entropy encoding, JPEG color stego Image.

Problem definition:
The cover image and the secret message are given. The objectives are

(i) Embed the secret message into the cover image to derive the stego image for security.

(ii) Improve PSNR between cover image and stego image.

(iii) Enhance the stego capacity.

Embedding algorithm:
In the embedding algorithm secret data is embedded into the cover image using segmentation into 16×16 non-overlapping blocks. The payload i-e secret data is embed into the quantized DCT coefficients after quantization.
Inputs: Colored Cover image 'C' and Secret Message 'M'
Output: Colored JPEG file

1. A cover image 'C' of any size like 256×256 is considered and any message such as character or strings is randomly generated for testing hiding algorithm.
2. Secret message is encrypted as data to be hidden it is in ASCII format which is converted to binary format.
3. Segmentation of cover image into blocks $\{C_1; C_2; C_3; \ldots ; C_N/16\times N/16\}$. Each Ci contains 16x16 pixels that are further transformed into DCT coefficients in transform domain.
4. DCT transforms each block Ci into DCT coefficient matrix Xi, where Xi = [a; b] = DCT (Ci [a;b]),
where $1\leq a; b \leq 16$ and Ci = [a; b] is the pixel value in Ci.
5. Application of new 16×16 modified quantization table 'T' that generates 136 Quantized AC coefficients.
6. Two secret bits with LSB method are embedded into least two significant bits of AC coefficients which correspond to the value 1 in quantization table.
7. Entropy coding is applied on color JPEG individual blocks of R, G and B which generates the required Compressed JPEG image file (Stego Image in Compressed Form).

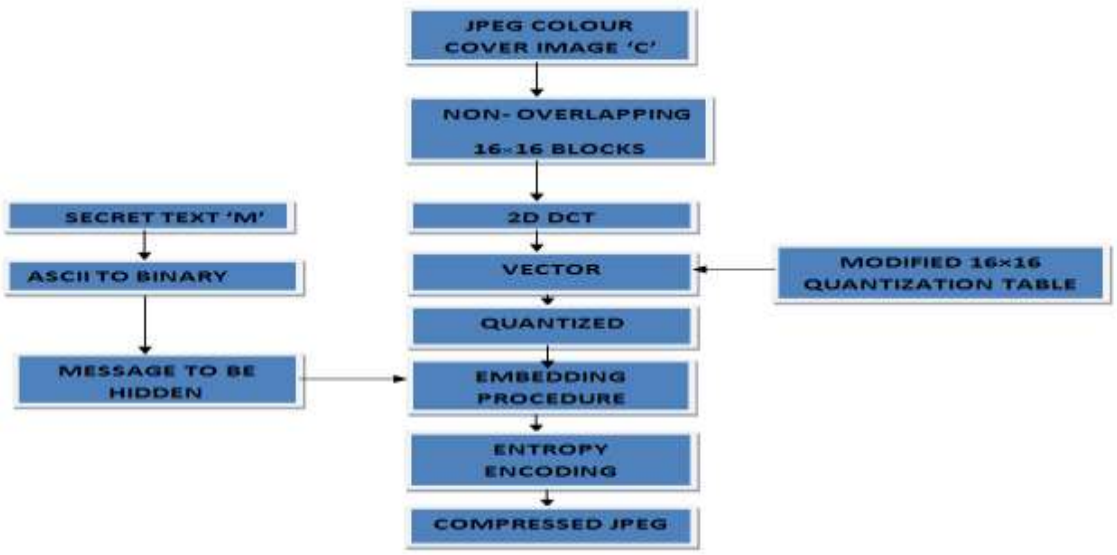

Figure 2: Embedding Procedure

Retrieving Algorithm:
The secret message is retrieved for the stego image by the adaptive reverse procedure of embedding and is given by as follows.
Input: Colored JPEG file
Output: Stego Image 'S' & Retrieved Secret Message 'M*'

1. Entropy decoding is done on the received JPEG image file.
2. Decoded block is followed by extraction of the secret message from least significant bits of 136 low and mid frequency coefficients .The message is decrypted to original ASCII format.
3. Dequantization using 16×16 quantization table is achieved.
4. Dequantized JPEG image is converted to spatial domain by implementing IDCT (Inverse Discrete cosine transform) segmented into 16×16 blocks.
5. Colored Stego Image obtained.
6. Secret Message 'M*' obtained.

M=Secret Text and M*=Extracted Secret Text

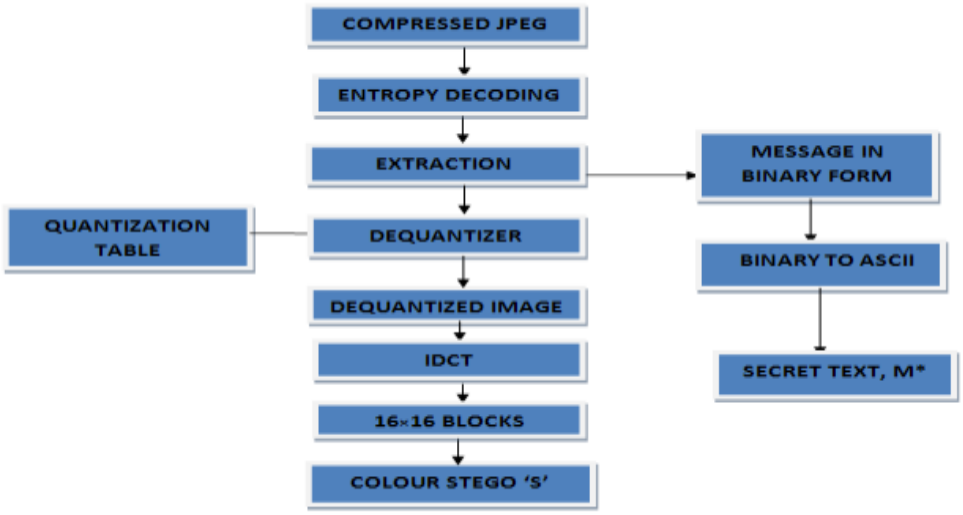

Figure 3: Extracting Procedure

IV. RESULTS AND DISCUSSION

Four color images, each of 256 x 256 and 512 x 512 pixels are used as test images. These cover images are Lena (1), Peppers (2), Jet (3), Baboon (4).

The steganographic methods used in this experiment were coded in Matlab R2008a (V 7.6.0) and run on a PC Pentium 4 with 1GB of RAM under the Windows XP operation system.GUI for steganography implementation using 16x16 quantized steganographic method has been shown in fig 5.

Lena (1) Pepper (2)

Jet (3) Baboon (4)

Figure 4: Test Images

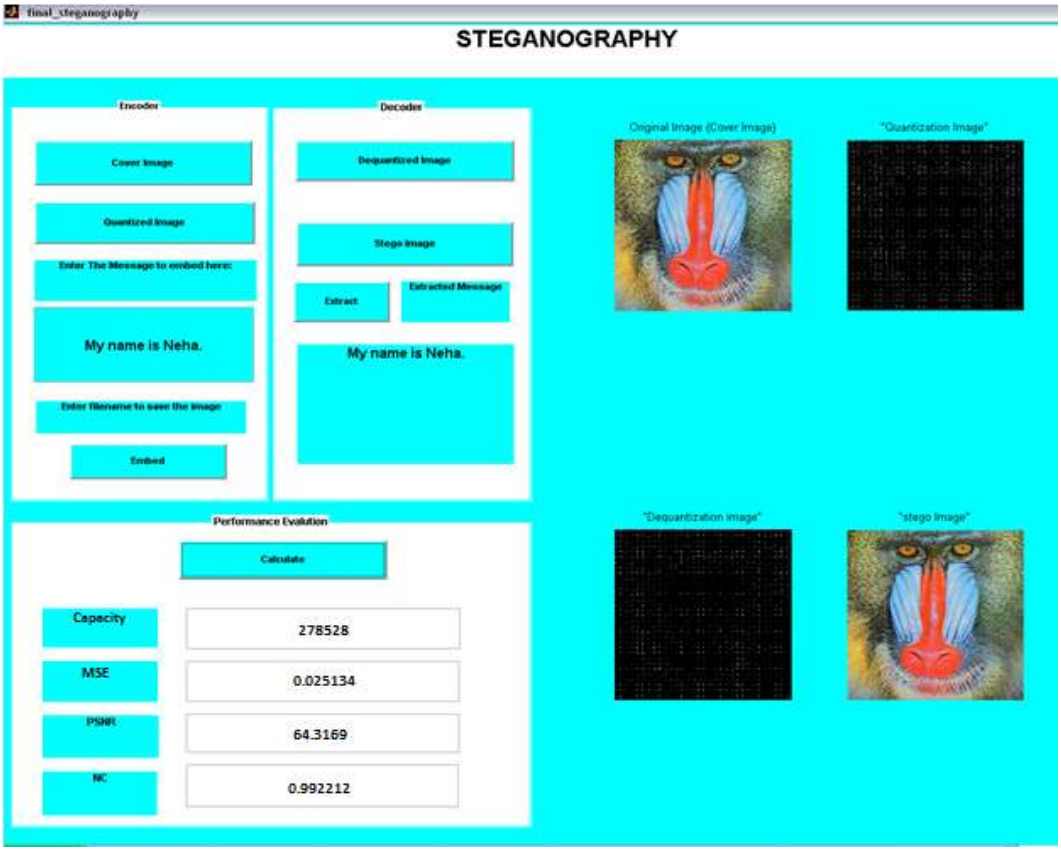

Figure 5: Graphical User Interface for image steganography showing both encoding and decoding process on Baboon Image as Cover Image (512x512 pixels)

First of all the image is browsed by clicking on cover image button. Quantized Image is obtained on the next click. Then the text that we have to hide "My name is Neha." in this case is written in the text box provided. Embed Button when pressed inserts the hidden message into the image. Then the button of GUI is clicked to get the stego image. Extract Button retrieves the hidden Message "My name is Neha". Calculate when clicked on gives the value of parameters like capacity and MSE, PSNR and NC.

TABLE I
COMPARISON OF HIDING CAPACITY, MSE , PSNR AND NC

S.No	Image	Pixels	Hiding Capacity(bits)	MSE	PSNR (db)	NC
1	Lena	256x256	69632	0.0981	58.2122	0.992176
		512x512	278528	0.0251	64.1282	0.992232
2	Pepper	256x256	69632	0.0931	56.9715	0.992181
		512x512	278528	0.025	62.2132	0.992252
3	Jet	256x256	69632	0.1771	55.6473	0.992185
		512x512	278528	0.0324	63.0185	0.992244
4	Baboon	256x256	69632	0.0944	58.3766	0.992141
		512x512	278528	0.024	64.3199	0.992212

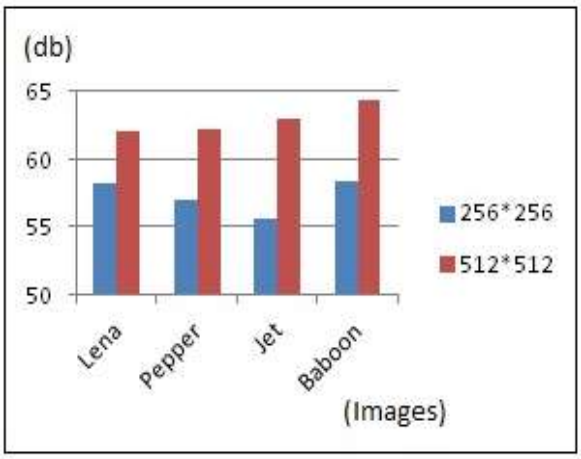

Fig 6: PSNR Comparison

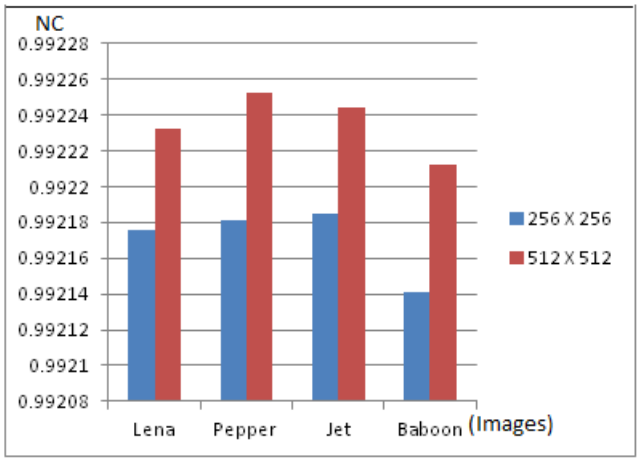

Fig 7: NC Comparison

TABLE II
COMPARISON OF STEGANOGRAPHY CAPACITY

Method	Lena	Baboon
Proposed	184757 bits	184757 bits
Chang Method	141284 bits	141284 bits
Jpeg-Jsteg	49798 bits	53142 bits

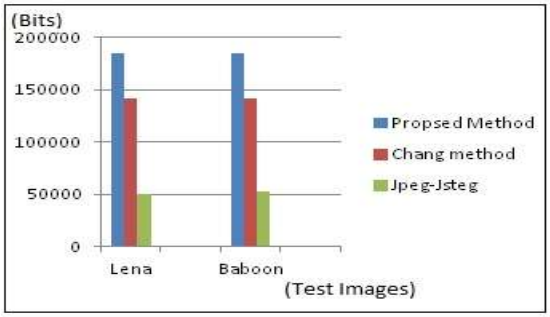

Fig 8: Capacity Comparison

V. CONCLUSION

In this paper, we implemented the proposed method with Four color images namely Lena, peppers, Jet, and Baboon as steganographic covers. Three parameters namely Capacity, MSE and PSNR have been compared on different sized test images. It has been found that capacity which is the amount of information embedding in color images increases as the number of modified quantized DCT coefficients increases. So more data can be embedded using of 16×16 Quantization Tables as compared to 8×8 tables. Table I indicates that 512 × 512 pixel image has more PSNR and less MSE as compared to 256×256 pixel images. Also it indicates that the cover image has high similarity (NC) to the stego image with higher pixel cover images.

Table II shows that our method has better capacity of embedding message bits in image than Jsteg and Chang's. Since the DCT coefficients after the quantization are almost all zeros, the message capacity of Jpeg–Jsteg is very much limited.

A block can embed can embed 136 × (417 × 417)/ (8 ×8) = 184757 secret bits into a cover image of 417 × 417 pixels.

In future, optimized quantization tables along with color transformation techniques can be used to increase the modified coefficients such as to have good capacity and PSNR values.

REFERENCES

[1] Monro D M ,Sherlock B G, "Optimal quantization strategy for DCT image signal processing", *IEEE Proceeding on Vision, Image and Signal Processing*.Vol.143,Issue-1,pp.10-14,1996.

[2] Huang J, Shi Y Q, Shi Y ,"Embedding image watermarks in DC components [J]",*IEEE Transactions on Circuits and Systems for Video Technology*.Vol.10,Issue-6,pp.974-979,2000.

[3] Lee Y K, Chen L H., "High capacity image steganograhic model [J]."*IEEE Proceedings on Vision, Image and Signal Processing*, Vol.147 (3), pp.288-294, 2000.

[4] Westfield A. "F5-a steganographic algorithm: high capacity despite better steganalysis[C]", *Proceeding of 4th International Workshop on Information Hiding*. New York: Springer-Verlag, pp.289-302, 2001.

[5] Ping Wah Wong; Memon, N, "Secret and public key image watermarking schemes for image authentication and ownership verification", *Image Processing, IEEE Transactions* on, Volume 10, Issue 10, 2001.

[6] Chang C C, Chen T S, Chung L Z. "A steganographic method based upon JPEG and quantization table modification [J]".*Information Sciences*, Vol.141, pp.123-138, 2002.

[7] Tseng H W, Chang C C. "Steganography using JPEG-compressed images [C]" *The Fourth International Conference on Computer and Information Technology*. Wuhan: IEEE Computer Society Press, pp.12-17, 2004.

[8] D.C. Lou and C.H. Sung, "A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem," *IEEE TRANSACTIONS ON MULTIMEDIA*, Vol. 6, No. 3, June 2004.

[9] K. Rabah, "Steganography-The Art of Hiding Data," *Information Technology Journal*, vol.3 (3), pp. 245-269, 2004, ISSN 1682-6027.

[10] Yu Y H, Chang C C, Hu Y C. "Hiding secret data in images via predictive coding [J]",*Pattern Recognition*, Vol.38,pp.691-705,2005.

[11] N.N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" *Journal of Computer Science*, vol.3 (4), pp. 223-232, 2007, ISSN 1549-3636.

[12] C.Y. Yang, "Color Image Steganography based on Module Substitutions," Third *International Conference on International Information Hiding and Multimedia Signal Processing* Year of Publication: 2007 ISBN: 0-7695-2994-1.

[13] Li Xiaoxia, Wang Jianjun. "A steganographic method based upon JPEG and particle swarm optimization algorithm". *Information Sciences*, Vol.177, 2007, 3099-3109.

[14] N. N. EL-Emam, "Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm," *International Journal of Information and Communication Engineering*, Vol.4, Issue-2, 2008.

[15] J.G.Yu1, E.J.Yoon2, S.H. Shin1 and K.Y. Yoo, "A New Image Steganography Based on 2k Correction and Edge-Detection", *Fifth International Conference on Information Technology*: New Generations 978-0-7695-3099-4/08, April 2008.

[16] W. Puech, M. Chaumont, and O. Strauss, ―A reversible data hiding method for encrypted images‖, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X. Edited by Delp, Edward J., III; Wong, Ping Wah; Dittmann, Jana; Memon, Nasir D. *Proceedings of the SPIE*, Volume 6819, pp.2-5,2008.

[17] Jiang cuiling, pang yilin, guo lun, jing bing, gong xiangyu. "A High Capacity Steganographic Method Based on Quantization Table Modification." *Wuhan University and Springer-Verlag Berlin Heidelberg*, Vol.16 No.3, pp.223-227, 2011.

Authors:

Neha Batra received her B.Tech. degree in Electronics & Comm. from Ambala College of engineering & Applied Research, Mithapur, Kurukshetra University, Haryana, in 2009 and is pursuing the M-Tech degree in Electronics & Communication from M.M. University, Mullana (Ambala). Presently, she is engaged in teaching, as a lecturer in Electronics & Comm. Department at Surya School of Engineering and Technology, Surya World, PTU.

Pooja Kaushik received her B.Tech. degree in Electronics & Comm. from Haryana College of Engineering Kurukshetra University, Haryana and M-Tech degree in Electronics & Comm. from M.M. University, Mullana (Ambala) . Presently, she is working as an Assistant Professor in Electronics & Comm. Department at M.M. University, Mullana (Ambala).