# Steganography Using 32*32 Vector Quantization Method in Color Image

**Rajni Goyal[1], Naresh Kumar[2]**
[1,2]Department of Computer Science & Engineering, Giani Zail Singh PTU Campus Bathinda, Punjab, India
[1]rajnigoyal88@gmail.com, [2]naresh2834@rediffmail.com

***Abstract*---In the present scenario, data security is one of the major challenges. 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. In this paper a text message is hidden into some colored image. We have used the function discrete cosine transform (DCT) and Vector Quantization method to quantize the image. Color image is taken for processing. A secret message of 128 characters can be embedded into the image. We have applied the 32*32 vector quantization as per the requirement. We will calculate the PSNR & NC of the given image. The result provide a better security and better PSNR & NC values.**

**Keywords—— DCT, PSNR, Steganography, vector quantization.**

## I. INTRODUCTION

Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it [1]. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. Cryptography is the method to hide secret data by scrambling so that it is unreadable, however it does not assure security and robustness as the hacker can obviously guess that there is a confidential message passing on from the source to the destination. The combination of cryptography and steganography provide high level security to the secrete information.[2]Cover image is known as carrier image and is the original image in which the secret data i.e., the payload is embedded. The unified image obtained after embedding the payload into the cover image is called the stego image. Image Steganography includes several techniques of hiding the payload within the cover image. Spatial Domain based Steganographic Techniques and Transform Domain based Steganographic Techniques. In this study we are using discrete cosine transform which is transformed domain based technique [3].

### *A. Related Work*

The two-dimensional DCT transform is used in steganography based on JPEG.The cover image is divided into non overlapping blocks of 8×8 pixels, then DCT transform is performed and the standard 8×8 quantization table is used to quantize each block. Jsteg is a well-known steganographic tool for its simple ideas and easy realization. It embeds the secret data in the LSB of each 8×8 block. But it embeds only one bit in each quantized coefficient so the capacity of this method is very limited.[3] On one hand, as the energy of the image is concentrated on the part of low frequency coefficients, modifying these coefficients will cause degradation of image quality. On the other hand, the high-frequency coefficients will be discarded in the quantization process. By using the embedding of middle frequency coefficients, Yu[4],Chang[5] and Tseng [6] proposed a modified 8×8 quantization table to increase the steganography capacity and achieve acceptable visual image quality. Based on Chang's quantization table proposed a method of dividing the cover image into non overlapping blocks of 16×16 pixels and gave a new quantization table, in which the quantization step size is half of Chang's**,** to reduce quantization error. Then, 2 bits of secret message are embedded in the LSB of every quantized middle frequency coefficients. Huang [7] proved the feasibility of embedding information in quantized DC coefficient through experiments.

## I. Technique Used

### A. *Discrete Cosine Transform(DCT*)

Discrete Cosine Transform (DCT) attempts to de correlate the image data. After de correlation each transform coefficient can be encoded independently without losing compression efficiency. The DCT is used in common image compression format MPEG or JPEG, wherein, the LSBs of the DCT coefficients of the cover image are replaced by the MSBs of the payload [4].

The One-Dimensional DCT

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right], \quad (1$$

The two-dimensional DCT

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right], \quad (2$$

### *B. Vector quantization*

Quantization is a process of representing a large possibly infinite set of values with a much smaller set. Color image quantization is a process that reduces the number of distinct colors used in an image, usually with the intention that the new image should be as visually similar as possible to the original image [7]. Scalar quantization is a mapping of an input value x into a finite number of output value y. Q: x → y Vector Quantization deals with quantizing the samples in groups called vectors. It is a lossy compression technique. It quantizes a number of input vectors together instead of one at a time [10].

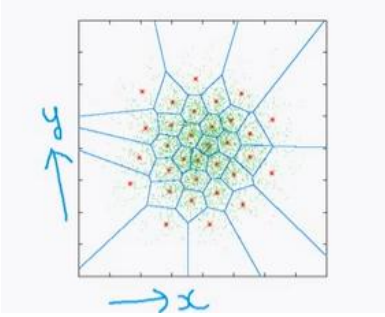



**Fig.**1 2-D example of vector Quantization

## II. EVALUATION PARAMETERS

Peak Signal to noise ratio (PSNR), Noise Capacity and Hiding Capacity as performance parameters to measure the quality of image [5].

a) **PSNR**–– It is measure of quality of image. PSNR can be calculated by using mathematically equation given below:

PSNR = 10*log10(peak^2/MSE);

b) **NC**–– it is the measure of noise in the stego image. It is calculated as.

NC= (signal*noise) / (signal*signal)

c) **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. It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic [1] embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage. It is calculated as

Capacity =2*136*(height*width) / (16*16);

## III. PROPOSED ALGORITHM

The procedure of embedding secret messages for JPEG-based steganography is illustrated as

1. The message to be embedded in the cover image is randomly generated, such as characters, images, or other information.
2. DCT transform is used after the cover image is divided into no overlapping blocks of 32*32 pixels. Then, the DCT coefficients are quantized by the new 32*32 quantization table
3. The message is embedded into the image by checking the proportion of red, green, blue color.
4. Then vector quantization method is applied to compress this.
5. The JPEG files will be transmitted to the receiver.
6. The secret message is taken out by the reverse process.

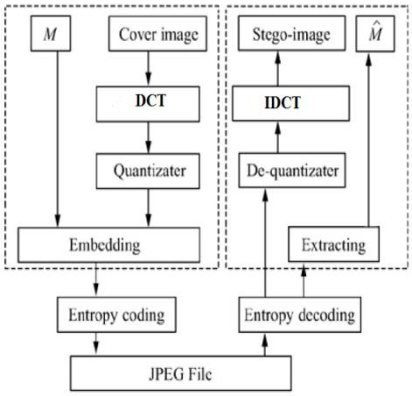



Fig.2 Process of Steganography

## IV. RESULTS & EVALUATIONS

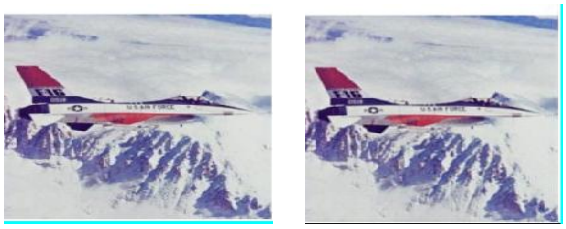
In Matlab, we conducted some experiments to evaluate the efficiency of our method. Three colored images Lena.jpg, peppers.jpg, and penguins.jpg of 512×512 pixels are used as cover images. The secret Message of size 128 characters is embedded. Most researchers use peak signal-to-noise ratio (PSNR) and mean square error (MSE) criteria to measure the quality of image. in the experiments. To further distinguish the degree of similarity between the cover image and stego image, we use the parameter NC

(a) (b)

**Fig.** 3 A simple image & Stego image for Lena

(a) (b)

**Fig.**4 A simple image & Stego image for Pepper



(a) (b)

**Fig.**5 A simple image & Stego image for plane

**TABLE I**

**PSNR VALUES FOR DIFFERENT IMAGES IN DIFFERENT METHOD**

| | PSNR Value | | |
|---|---|---|---|
| **Image** | **Lena** | **plane** | **Pepper** |
| Jsteg method | 36.85 | 36.00 | 36.27 |
| Chang's method | 43.44 | 43.51 | 42.63 |
| Quantization table Modification method | 46.44 | 46.03 | 45.15 |
| Our proposed method | 66.38 | 55.00 | 63.01 |

**TABLE II**

**NC VALUES FOR DIFFERENT IMAGES IN DIFFERENT METHODS**

| | NC Value | | |
|---|---|---|---|
| **Image** | **Lena** | **Pepper** | **Plane** |
| Jsteg method | 0.9983 | 0.9982 | 0.9985 |
| Chang's method | 0.9999 | 0.9998 | 0.9999 |
| Quantization table Modification method | 0.9997 | 0.9998 | 0.9997 |
| Our proposed method | 0.9921 | 0.9921 | 0.9922 |

## V. CONCLUSION & FUTURE SCOPE

From the work which we have done, we can conclude that 32 * 32 vector quantization is a very efficient technique for the image stegnography if it is combined with DCT & IDCT technique. The only drawback in this current research work is that there is no looping method in the entire section through which the blocks can check out that whether there is any other possibility to merge the message bits more, although the results which have come out from our method are quite effective but still modifications are always possible. In future if someone can try his hands over Neural, it might provide some better results.

## REFERENCES

**[1]** V.K Maan and H.S Dhaliwal," Vector Quantization In Image Steganography," International Journal of Engineering Research & Technology, Vol. 2 Issue 4, pp.421-424, April 2013.

**[2]** M. Paul and J. K Mandal," A Universal Session Based Bit Level Symmetric Key Cryptographic Technique to Enhance the Information Security" International Journal of Network Security & Its Applications , Vol.4, No.4, pp.123-136, July 2012.

**[3]** J.Cuiling, P.Yilin, G.Lun, and J.Bing,"A High Capacity Steganographic Method Based on Quantization Table Modification," Wuhan university journal of natural science, Vol.16 No.3,pp. 223-227,July 2011.

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

**[5]** C.Chang, T.S Chen and L.Z Chung,"A steganographic method based upon JPEG and quantization table modification" InformationSciences, pp.123-138, 2002.

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

**[7]** Y. K Lee and L.H Chen,"High capacity image steganographic model,"IEEE Proceedings on Vision, Image and Signal Processing,pp. 288-294. 2000.

**[8]** A.Ahmed and Abdelwahab," A New Image Steganography Technique" Journal of Engineering and

Computer Sciences, Qassim University, Vol. 1, No. 2, pp. 109-117,July 2008

**[9]** A. Skodras, C. Christopoulos, and T. Ebrahimi "The JPEG 2000 Still Image Compression Standard" IEEE Signal Processing Magazine,pp.1053-1064, 2001.

**[10]** Z.M.Lu, J.S Pan and S.H Sun, "Image Coding Based on classified sidematch vector quantization," IEICE Trans. Inf. & Sys., vol.E83-D (12), pp.2189-2192, Dec. 2000.

**[11]** R. M. Gray, "Vector quantization," IEEE Acoustics, speech and Signal Processing Magazine, pp. 4-29, 1984.

**[12]** L. Xiaoxia and W. Jianjun," A steganographic method based upon JPEG and particle swarm optimaziton algorithm,".Information Sciences, pp.3099-3109, 2007