INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

STEGANOGRAPHY ON COLOUR IMAGES USING 32X32 QUANTIZATION TABLE

Tara Bansal[1], Ruchika Lamba[2]

[1]Department of Electrical and Instrumentation Engineering, Thapar University
Patiala, 147004, Punjab, India
tarabansale63@gmail.com

[2]Department of Electrical and Instrumentation Engineering, Thapar University
Patiala, 147004, Punjab, India
ruchika.mehta@thapar.edu

Abstract: *Steganography is hiding private or secret data within a carrier in invisible manner. Steganography refers to the information that has been concealed inside a digital picture, video or audio file. This paper is based on JPEG quantization table modification. Firstly, the cover image is divided into 32*32 blocks and DCT is applied on each block. The number of payload LSB bits is embedded into DCT coefficients of the cover image based on the values of DCT coefficients. Secondly, IDCT is applied to produce the stego image which is identical to cover image. Then, the watermarked image is transmitted over the public channel. Our basis objective is to work on the color images with three planes and to work out on the Capacity, PSNR AND MSE values.*

Key Words: *Steganography, Capacity, MSE, PSNR, DCT, IDCT.*

1. INTRODUCTION

Steganography is a means of establishing secret communication through public channel in an artistic manner. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing”[1] defining it as “covered writing”. In image steganography the information is hidden exclusively in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. 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. Capacity, security, and robustness [3] are the three different aspects contended with each other in the information hiding systems.

Image steganography is about exploiting the limited power of the human visual system (HVS). If any specific colour is viewed closely it has been observed that single digit modifications to the contribution level are imperceptible to the human eye (i.e. a pixel with a value of (255, 255, 0) is indistinguishable from (254, 255, 0)) in RGB colour representation. LSB techniques [4] are used to reduce the data to a suitable size in order to display it in a reasonable amount of time across the Internet. This technique called compression makes use of some mathematical concepts to reduce the image data, resulting in smaller file sizes and plays a vital role in image based steganography methods. Hash based least significant bit (LSB) has been proposed [5] in which a spatial domain technique is used where the secret information is embedded in the LSB of the cover frames. Image Fidelity (IF) is also measured and the results show minimal degradation of the steganographic video file. High capacity steganographic approach based on Discrete Cosine Transformation (DCT) and JPEG compression [6] has been proposed. Some difficulties are pointed out that stand in the way of a theory of “perfect covertness" with the same power as Shannon's theory of perfect secrecy. But considerations of entropy give us some quantitative leverage and the “selection channel" the bandwidth of the stego key led us to suggest embedding information in parity checks rather than in the data directly. This approach gives improved efficiency, and also allows us to do public key steganography [7].

2. RELATED WORK

The proposed technique is based on Segmentation, Discrete Cosine Transform and Watermarking. The cover image is divided into 8*8 blocks and DCT is applied on each block. The number of payload MSB

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

bits is embedded into DCT coefficients of the cover image based on the values of DCT coefficients. Finally the watermarked image is transmitted over the public channel.

- To segment the cover image into 8*8 blocks
- To apply DCT on each block to get the DCT coefficients
- To find the bit length to hide the data
- To embed the data in DCT coefficients according to the bit length
- To apply IDCT in order to get the stego image in spatial domain
- To add the watermark in the obtained stego image, to protect it from intruder
- To extract watermark and the stego image
- To evaluate the image using parameters like MSE, PSNR and capacity.

3. PROPOSED WORK

3.1. Algorithms:

The model uses an adaptive data hiding technique, where the number of payload bits *L* is embedded into the DCT coefficient of cover image based on the DCT coefficient of cover image in order to maximize the hiding capacity. The payload is embedded into the cover image by segmentation, DCT and adaptive bit length L.

3.1.1 Embedding Algorithm:

The cover image is segmented into 8x8 matrices. The DCT is applied on each 8x8 block to get DCT coefficients which are used to hide the payload Most Significant Bit (MSB) based on the DCT coefficient values of the cover image. Transform each 8x8 matrix into frequency domain using 2D-DCT. Four MSBs of each payload pixel are embedded into the cover image DCT coefficients in a continuous manner depends on the value of *L* to derive the stego image in DCT domain. The stego image in the transform domain is converted to the spatial domain by applying IDCT. The stego image obtained is similar to the cover image and the difference is not perceptible by the human eye. The watermark is added to the stego image to make it protected. This watermarked image is transmitted to the destination over the open channel.

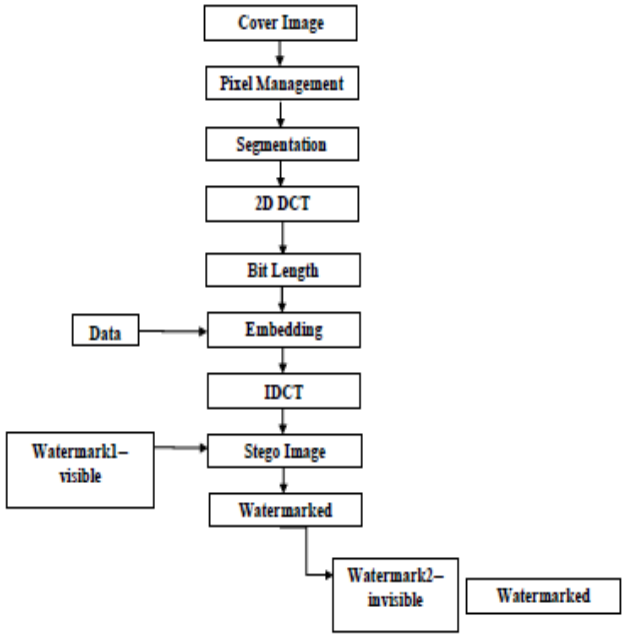

Figure 3.1.1.1: Block Diagram of Embedding Technique [8].

3.1.2 Retrieval Algorithm

The watermarked image is received at the destination over the open channel. Any intruder interfering in the transmission process will only be able to read the watermarked image and cannot extract the secret data embedded in it. The watermarked will be removed first of all to get the stego image, and then this stego image is segmented into 8x8 blocks to ensure proper retrieval of data. The 8x8 sub blocks of stego image are transformed into frequency domain to generate DCT coefficients using 2D-DCT.

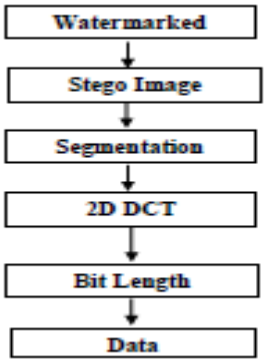

Figure 3.1.2.1: Block Diagram of Retrieval Technique [8]

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

.3.2. Evaluation Parameters

3.2.1 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 steganographic 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 [8].

3.2.2 Mean Square Error (MSE)

It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE [8]. It is calculated using Equation 1:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

I (i,j) = The intensity value of the pixel in the cover image.
K (i,j) = The intensity value of the pixel in the stego image.
m*n = Dimensions of image.

3.2.3 Peak Signal to Noise Ratio (PSNR)

It is the measure of quality of the image by comparing the cover image with the stego image, i.e. it measures the percentage of the stegano data to the image percentage [8]. PSNR is calculated Equation 2:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

4. RESULTS

Five color images, each of 256 x 256 and 512 x 512 pixels are used as test images. These cover images are Baboon (1), Koala (2), Lena (3) Penguins (4) Pepper (5).

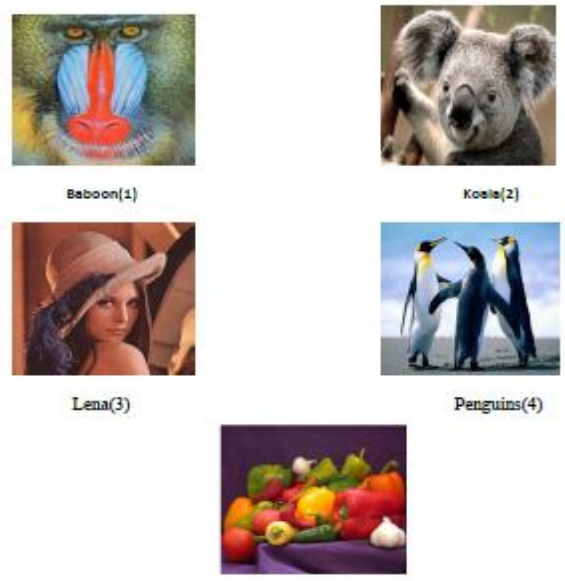

Figure 4.1: Test images

Graphical User Interface GUI for steganography implementation using 32x32 quantized steganographic methods has been shown in fig 4.2.

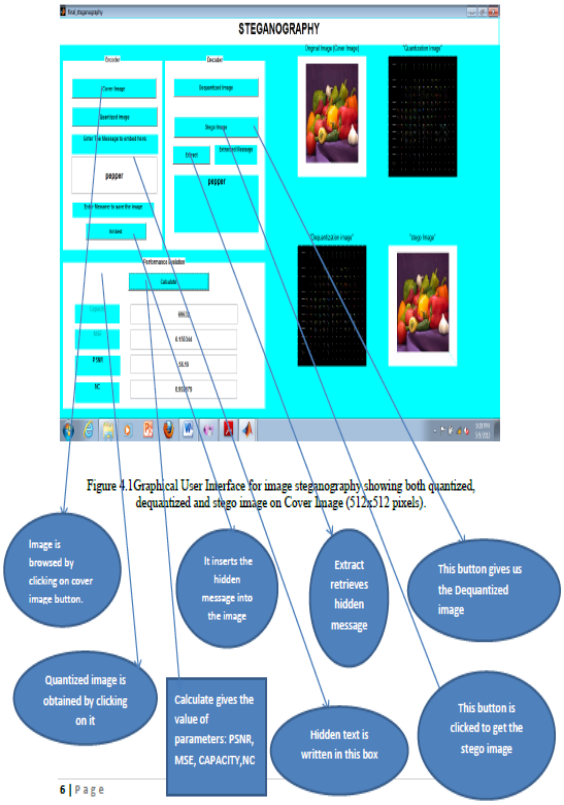

Figure 4.1Graphical User Interface for image steganography showing both quantized, dequantized and stego image on Cover Image (512x512 pixels).

Figure 4.2

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

TABLE 1: Comparison of Hiding Capacity, MSE, PSNR

IMAGE	PIXEL	HIDING CAPACITY (Bits)	MSE	PSNR (db)
1.Baboon	256x256	69632	0.0961214	58.3026
	512x512	278528	0.0240604	64.3178
2.Koala	256x256	69632	0.0845769	58.8583
	512x512	278528	0.0211915	64.8692
3.Lena	256x256	69632	0.0596887	60.3719
	512x512	278528	0.0149363	66.3884
4.Peguins	256x256	69632	0.143417	56.5648
	512x512	278528	0.0359311	62.5761
5.Peppers	256x256	69632	0.156344	56.19
	512x512	278528	0.0391673	62.2016

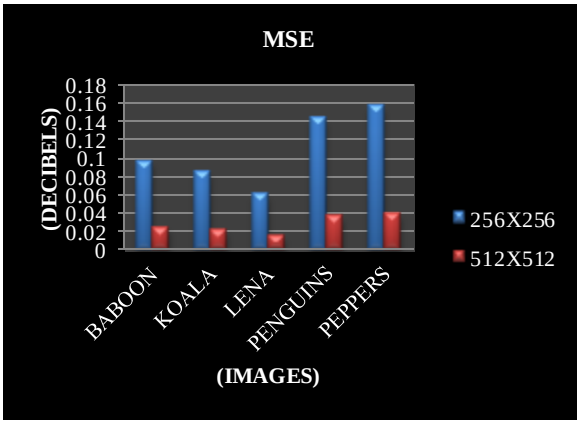

Figure4.2: MSE Comparison

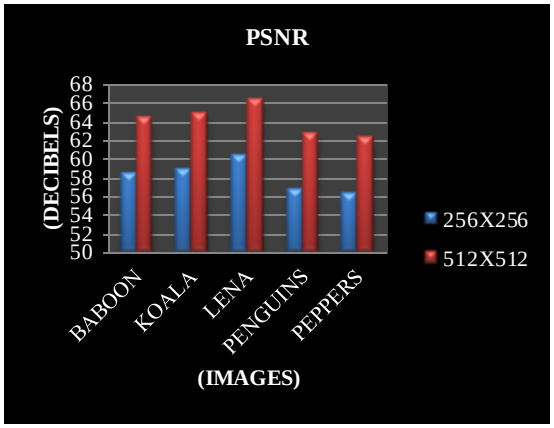

Figure 4.3: PSNR Comparison

5. CONCLUSION

In this paper, we implemented the proposed method with five colour images namely Lena, peppers, penguins and koala, and Baboon as steganographic covers. We have compared 3 parameters namely PSNR, MSE, Capacity on different test images using 32x32 Quantization. It has been found that 512x512 pixel images has more PSNR and Capacity as compared to 256x256 and 512X512 pixel image has less MSE as compared to 256x256 pixel image.

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

REFERENCES

[1] Secret and public key image watermarking schemes for image authentication and ownership verification by Ping Wah Wong, Memon, N, IEEE Transactions on, Volume 10, Issue 10, 2001.

[2] Implementation of Modified 16×16 Quantization Table Steganography on Colour Images by Neha Batra, Pooja Kaushik, and International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012

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

[4] High capacity data hiding using LSB Steganography and encryption by Shamim Ahmed

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Laskar and Kattamanchi Hemachandran, International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

[5] Hash based least significant bit technique for Video Steganography (HLSB) by Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, International Journal of Security, Privacy and Trust Management IJSPTM), Vol. 1, No 2, April 2012.

[6] High capacity Steganographic method based upon JPEG by Adel Almohammad Robert M. Hierons, The Third International Conference on Availability, Reliability and Security.

[7] On the limits of Steganography by Ross J. Anderson, Fabien A.P. Petitcolas, IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

[8] Bit length replacement Steganography based on DCT coefficients by K B Shiva Kumar, K B Raja, R K Chhotaray, Sabyasachi Pattanaik, International Journal of Engineering Science and Technology Vol. 2(8), 2010, 3561-3570.