32×32 Colour Image Steganography

Veerdeep Kaur Mann[1], Harmanjot Singh Dhaliwal[2]

[1]Student, M.Tech ECE,UCOE, Punjabi University Patiala
[2]Assistant Professor, UCOE, ECE, Punjabi University Patiala

Abstract— ***The word steganography is originally derived from Greek words which mean "Hidden Writing".Due to the rapid growth of usage of internet over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography. 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. In this paper we worked on quality of stego-image. Stego image should have better data embedding capacity and should have small computational time.***

Keywords—**Steganography,DCT,IDCT,Cryptography.**

I. INTRODUCTION

Images can be more than what we see with our Human Visual System (HVS), means they can convey more than 1000 words. The objective of the steganography is to hiding the embedded information into the image such that the existence of the embedded message in the image is imperceptible to the human beings . Due to the rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography. The word steganography is originally derived from Greek words which mean "Hidden Writing". Steganography has evolved into a digital strategy of hiding a file in some form of an image, an audio file or even a video file.

A steganography system is expected to meet three key requirements, namely transparency, capacity and robustness.

Transparency: Transparency evaluates the image distortion due to signal modifications like message embedding or attacking.

Capacity: It is the maximum amount of information that a data hiding scheme can successfully embed without introducing any perceptual distortion in the marked media.

Robustness: Robustness measures the ability of embedded data or watermark to withstand against intentional and unintentional attacks.

So, Steganography is the method through which existence of the message can be kept secret. This is accomplished through hiding information in another information, thus hiding the existence of the communicated information.

Techniques related to steganography are Cryptography watermarking and fingerprinting.While, Cryptography is the science of using mathematics to encrypt and decrypt data ,means cryptography is the science of securing data with encryption and decryption methods. It enable to store sensitive(secure) information through insecure network. The information transmitted will only be read by the intended recipient. Within the context of any application-to-application communication authentication, privacy ,integrity and non-repudiation are some specific security requirements. Watermarking-A digital watermark is a pattern of bits inserted into a digital file - image, audio or video. Such messages usually carry copyright information of the file. Digital watermarking technology has many applications in protection, certification, distribution, anti-counterfeit of the digital media and label of the user information [1]. With fingerprinting , different or unique marks are embedded in different copies of the carrier object that are supplied to different customers. This enables the owner to identify those customers who break their licensing agreement by supplying the property to some other parties.

Steganography is a technique 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 To hide information, straight message insertion scheme may encode every bit of information in na dalso may selectively embed the message in "noisy" areas that draw less attention in those areas where there is a great deal of natural colour variation. The embedded message may also be scattered randomly throughout the image. There are number of ways exist to hide information in digital media. The most common approaches include:-

1) Least significant bit insertion
2) Masking and filtering
3) Redundant Pattern Encoding
4) Encrypt and Scatter
5) Algorithms and transformations

Each of these techniques can be applied, with distinct degrees of success [2].

For the image steganography, there are two types of domains, one is spatial domain method and other is frequency domain method. For the spatial domain method, the secret messages will be hidden in the pixels of cover image ([3]-[4]). As in Chan et al.'s research, data was hidden by
using simple least significant bit methods with an optimal pixel adjustment process [3]. But in case of the frequency domain method ,firstly the cover image be transformed from spatial domain to frequency domain before embedding the secret messages ([5]-[7]). In addition, for the spatial domain method the capacity of the secret messages that can be embedded is greater than that of frequency domain method, however, it is easier to be detected with the Human Vision System.

In this work, frequency domain method is chosen. Initially, the transformation from spatial domain to frequency domain is applied to an image with the advantage of the characteristic of our Human Vision System which is sensitive

to the low frequency range and insensitive to high frequency range. Once the image is transformed into frequency domain, the high frequency range can be discarded. In addition, there are various transform techniques used in steganography works such as DCT [5-6], DFT [8] and DWT [7] However, many image algorithms use DCT because unlike DFT, there is no need to work with the imaginary part. In this work, DCT is used to transform cover image into frequency domain. Also, the image file format used in this paper is based on JPEG. The advantage of JPEG is its compression efficiency in high quality. With this reason, it is widely used over the internet. Therefore, using JPEG as our image format file will reduce the chance to be suspected.

For this work, we had considered four significant factors which are 1-capacity of the secret messages that can be embedded, 2-quality of the stego-image i,e stego-image and cover-image should be quite similar such that the difference is not detected by our human visual system. If more secret messages can be embedded but the quality is degraded such that it can easily be detected, 3-stego-image's size if the size is increased too much then it can easily be suspected and 4-computational time, if more secret messages can be embedded and the quality is good but the computational time is significantly increased then it would not be practical used. Therefore, for this work, the considered factors are quite important for secret communication.

This paper consists of five sections starting with the introduction. Section 2 reviews about the related work. Section 3 reviews the design and developmentof this work. Furthermore, Section 4 is about our experimental results... Finally, the conclusion will be in the Section 5.

II RELATED WORK

M.H. Lin, Y.C. Hu, C.C. Chang in 2002 used a true color secret image and their requirement was a large number of storage and bandwidth during transmission. To reduce the size of the transmitted data, the secret image was quantized. The method of color quantization employed in this scheme was uniform quantization, in which the red, green, and blue components of the secret image are coarsely quantized. This scheme provided a method for hiding both true color and grayscale secret images. However, the quality of the extracted color secret image was not good in terms of the peak signal-to-noise ratio (PSNR) value and visual observation. As the method of color quantization was employed in their scheme was fixed color quantization and the secret image was coarsely quantized, which was unable to preserve the color information of an image [9].

Yuan-Hui Yu , Chin-Chen Chang , Iuon-Chang Lin c in November 2006 proposed a new steganographic method for embedding a color or a grayscale image in a true color image while providing high hiding capacity and retaining high image quality. There are three types of hiding in the proposed method: hiding a color secret image in a true color image, hiding a palette-based 256-color secret image in a true color image, and hiding a grayscale image in a true color image. The image quality was better than that of the scheme of M.H. Lin, Y.C. Hu, C.C. Chang . The PSNR values of the stego-images and the retrieved secret images were all higher. The hiding capacity of the proposed method is greater than that of other compared schemes. Overall, the proposed method is a secure steganographic method providing high hiding capacity and high image quality [10].

Adel Almohammad , Gheorghita Ghinea and Robert M. Hierons in 2009 proposed a High Capacity Steganographic Method Based Upon the JPEG standard which uses 8x8 quantization tables, but it does not specify any default or standard values for quantization tables. However, the JPEG standard provides a pair of quantization tables as examples tested empirically and found to generate good results. Dividing this quantization table they get a new quantization table . Using this new quantization table generates reconstructed images almost identical to the source image . Therefore, this table will be used with Jpeg-Jsteg method in the experiment. Since the values of these tables could be an arbitrary choice , some researchers modified these quantization tables for their research purposes. A quantization table can arbitrarily be generated. Consequently, They produced a 16x16 quantization table by simulating and stretching the scaled quantization table [11].

Neha Batra Pooja Kaushik in October 2012 suggested a steganographic method based upon blocks of 16x16 pixels and modified 16x16 quantization table. Therefore, they used the same technique used by Chang et al. However, they divide the cover image into non-overlapping blocks of 16x16 pixels and used larger quantization table in order to improve the embedding capacity in colour images. They had considered colour images and investigated their feasibility of data hiding. Three performance parameters namely Capacity, Mean Square Error and Peak Signal to Noise Ratio have been compared on different sizes of standard test images. In comparison to Jpeg-Jsteg and Chang et al, the proposed method showed high performance with regard to embedding rate and PSNR of stego image. Furthermore, the produced stego-images were almost identical to the original cover images. It also had been found that capacity which is the amount of information embedding in colour images increases as the number of modified quantized DCT coefficients increases. So capacity was also increased as more data can be embedded using of 16×16 Quantization Tables as compared to 8×8 tables [12].

Natee Vongurai and Suphakant Phimoltares in 2012 proposed a new technique in which Instead of using 8x8-pixel blocks with the 8x8-pixel quantization table, a larger block of size 32x32 was used with a corresponding 32x32 quantization table created by cubic interpolation technique. Grey scale images were used. They used the frequency based image steganography using Discrete Cosine Transformation (DCT) which prodeced reduction of computation time and increased the capacity of the secret messages while maintaining the image quality and the size of JPEG stego-image. The transformation from spatial domain to frequency domain was applied to an image with the advantage of the characteristic of HVS (Human Vision System) that is sensitive to the low frequency range and insensitive to high frequency range. As

the image was transformed into frequency domain, the high frequency range was discarded. The experiments were conducted and comparisons were done with Chang's and Almohammad's methods and results has less computation time and increase the capacity while maintaining the size and image quality[13].

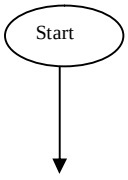
III DESIGN and DEVOLPMENT

Image Steganography includes several techniques of hiding the payload within the cover image. The most popular hiding techniques are Transform Domain based Steganographic Techniques and Spatial Domain based Steganographic Techniques . Spatial domain based steganography includes the Least Significant Bit (LSB) technique, Most Significant Bit (MSB) technique and Bit Plane Complexity Steganographic (BPCS) technique. In transform domain the cover image or the payload is transformed into frequency domain by using Fast Fourier Transform, DCT, Discrete Wavelet Transform (DWT) and Integer Wavelet Transform. In our proporsed work spatial domain and frequency domain techniques are used for both encoding and decoding of the images. We used DCT and IDCT method so that the output image (stego-image) similar to the input image (cover image). There are several different techniques used for the encoding of images. In our proposed work , we have tried to combine all of the above works along with the previously done works.The original aim of this work is to increase stego image quality and compare the result with previous work done. In our proposed work first of all we have taken different images . First of all we upload the image, we would process the image accordingly .We have used the VQ method. Vector Quantization (VQ) is one of the techniques based on the principle of block coding that have long been used to compress media in order to make efficient use of network bandwidth and data storage space.

The proposed method consist of six stages:-

1) Firstly, the image is uploaded.
2) VQ method is applied to segment the cover image into 32*32 blocks.
3) Apply DCT on each block to get the DCT coefficients to find the bit length to hide the data.
4) To embed the data in DCT coefficients according to the bit length.
5) Apply IDCT in order to get the stego image and compare the stego image and cover image.
6) Evaluate the parameters.

System Flowchart



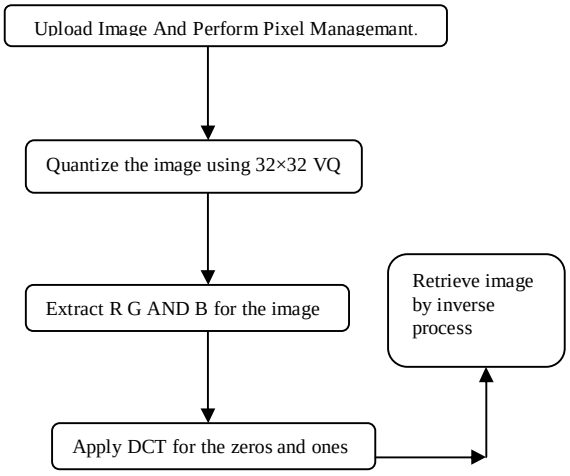


Fig. System flow chart

IV EXPERIMENTAL RESULTS

In our proposed work we have applied a strong blocking scheme in which the result of one encoding scheme goes to another block. In certain manner we have used the following blocks:-

1) Uploading of cover image.
2) Quantization block.
3) Data embedding block.
4) DCT block.

With each and every block of processing the encoding goes strong and strong enough to be decoded easily. In the first proceeding , we upload the colour image of leena

Our experiments are executed on MATLAB R2010B windows 7, CPU Core i5 with 2 GB of ram. two 512x512-pixel colour images of Lena and Pepper are used as cover images. Four criteria, consisting of 1) capacity of the secret messages that can be embedded, 2) quality of the stego-image, 3) size of the stego-image, and 4) the computational time consumed during the process, are used to measure the performance of our method.

1) *Peak Signal to Noise Ratio (PSNR)*

It is the measure of quality of the image by comparing the cover image with the stego-image,. PSNR is calculated Equation below:-

$$PSNR=10.\log_{10}\left(\frac{MAX^2}{MSE}\right)$$

$$=20.\log_{10}\left(\frac{MAX^2}{\sqrt{MSE}}\right)$$

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. It is calculated using Equation below:-

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

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 steganographic embedding operation needs to preserve the statistical and perceptual quality of the cover image. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage.

4)Computational time:-

It is the total time consumed for the retrieval of the image which has been embedded into the base image.

Images used as cover images are given below

Lena(1) college(2) flower(3)



Penguins(4) pot(5)


Calculated parameters of the Stego-Images (DB)

Our	*Image of size 1024×1024*

Method	*Psnr*	*MSE*	*Capacity*	*Time*
Lena	72.4627	0.00368817	1.11411e+006	0.14278
college	70.9717	0.00519884	1.11411e+006	0.1435
flower	67.7439	0.0109317	1.11411e+006	0.14523
penguins	68.5992	0.0089776	1.11411e+006	0.15902
Pot	67.4934	0.0115809	1.11411e+006	0.14712

TABLE 1

V CONCLUSION

In this paper, we implemented the proposed method on five colour images namely Lena, college, flower, penguins and pot as steganographic cover images. We had calculated four parameters namely PSNR, MSE, Capacity and time (computational time) in table 1 on different test images using 32x32 Quantization. It has been found that 1024×1024 pixel images. 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 results which we have concluded are quite improved from the previous work.

References

[1] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques.

[2] A Tutorial Review on Steganography Samir K Bandyopadhyay, Debnath Bhattacharyya ,Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, IC3–2008 UFL & JIITU.

[3] P.Nithyanandam, T.Ravichandran, N.M.Santron and E.Priyadarshini, "A spatial domain image steganography technique based on matrix embedding and huffman encoding," Int. J. of Computer Science and Security, vol. 5 , issue 5, 2011, pp. 456-468.

[4] C.-K. Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, issue 3, pp. 469 – 474, March 2004.

[5] C.-C. Chang ,T.-S. Chen, L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification," Information Science, vol. 141, issue 1-2, pp. 123-138, March 2002.

[6] A. Almohammad, R. M. Hierons, G. Ghinea, "High capacity steganographic method based upon JPEG," IEEE 3rd Int. Conf. on Availability, Reliability and Security, 2008, pp. 544-549.

[7] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, "A novel technique for image steganography based on DWT and huffman encoding," Int. J. of Computer Science and Security, vol. 4, issue 6, 2011, pp. 561-570

[8] F. Alturki ,R. Mersereau, "Secure blind image steganographic technique using Discrete Fourier Transformation." IEEE Proc. Int. Conf. on Image Processing, 2001, vol. 2, pp. 542-545.

[9] M.H. Lin, Y.C. Hu, C.C. Chang, Both color and gray scale secret images hiding in a color image, International Journal of Pattern Recognition and Artificial Intelligence 16 (2002) ,pp.697–713.

[10] Yuan-Hui Yu a,*, Chin-Chen Chang b, Iuon-Chang Lin c,"A new steganographic method for color and grayscale image hiding Received 16 March 2006; accepted 4 November 2006.

[11] Adel Almohammad Robert M. Hierons" High Capacity Steganographic Method Based Upon JPEG The Third International Conference on Availability, Reliability and Security, June 21, 2009.

[12] Neha Batra Pooja Kaushik" Implementation of Modified 16×16 Quantization Table Steganography on Colour Images,Volume 2, Issue 10, October 2012 ISSN: 2277 128X.

[13] Natee Vongurai and Suphakant Phimoltares", Frequency-Based Steganography Using 32x32 Interpolated Quantization Table and Discrete Cosine Transform, 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation, 2166-8531/12.