International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 2 Issue 9, September-2013, pp: (28-33), Available online at: www.erpublications.com

32×32 Vector Quantization Based Colour Image Steganography

Veerdeep Kaur Maan[1], Harmanjot Singh Dhaliwal[2]
[1]M.Tech. Scholar, [2]Asst. Professor,
UCOE, ECE, Punjabi University Patiala, Punjab, India

Abstract: Image Steganography is the art of hiding information into a cover image. Our approach involves Image steganography based on DCT AND DWT, where DCT- DWT is used to transform original image (cover image) from spatial domain to frequency domain. The objective of steganography is hiding the embedded message into the cover image such that the existence of embedded message in the cover image is imperceptible to the human beings. In this paper we worked on quality of stego-image by working out on psnr, mse, capacity, computational time.

Keywords: Steganography, DCT, IDCT, DWT, Cryptography.

I. INTRODUCTION

The 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 hiding 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 "Covered 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. 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: Capacity of an information hiding scheme refers to the amount of infonnation that a data hiding scheme can successfully embed without introducing 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. There are number of ways exist to hide information in digital media. 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 varying degrees of success [2].

1) Least significant bit (LSB) method

This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message [3] . Security measures have become very necessary issue in the age of digital transmission of information via Internet. Two schemes are used to protect secret messages from being captured during transmission. One is encryption where the secret information is encoded in another form by using a secret key before sending, which can only be decoded with secret keys. The most popular encryption techniques are DES, RSA etc. Other way is steganography which is a technique of hiding secret information into a cover media or carrier. If the cover media is a digital image, it is called cover image and the cover image with hidden data is called stego-image.

2) Masking and filtering techniques

Masking and filtering techniques usually restricted to 24 bits and gray scale images hide information by marking an image, in a manner similar to paper watermarks [4]. The techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing. This makes it more suitable than LSB with, for instance, lossy JPEG images.

3) Redundant Pattern Encoding

Patchwork and other similar tools do redundant pattern encoding, which is a sort of spread spectrum technique. It works by scattering the message throughout the picture. This makes the image more resistant to cropping and rotation. Smaller secret images work better to increase the redundancy embedded in the cover image, and thus make it easier to recover if the stego-image is manipulated [5].

4) Encrypt and Scatter

The Encrypt and Scatter technique tries to emulate white noise. It is mostly used in image steganography. White Noise Storm is one such program that employs spread spectrum and frequency hopping. It does this by scattering the message throughout an image on eight channels within a random number that is generated by the previous window size and data channel. The channels then swap rotate, and interlace amongst each other. Each channel represents one bit and as a result there are many unaffected bits in each channel. This technique is a lot harder to extract a message out of than an LSB scheme because to decode firstly detect that a hidden image exists and extract the bit pattern from the file. While that is true for any stego-image you will also need the algorithm and stego key to decode the bit pattern, both of which are not required to recover a message from LSB. Some people prefer this method due to the considerable amount of extra effort that someone without the algorithm and stego-key would have to go through to extract the message. Even though White Noise Storm provides extra security against message extraction it is just as susceptible as straight LSB to image degradation due to image processing [6].

5) Algorithms and transformations

The transformation from spatial domain to frequency domain are 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. 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, DFT and DWT. However, many image algorithms use DCT because unlike DFT, there is no need to work with the imaginary part. Also, the image file formats commonly used are 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 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 ([7]-[8]). As in Chan et al.'s research, data was hidden by using simple least significant bit methods with an optimal pixel adjustment process [7]. 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 ([9]-[10]). 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, DFT and DWT. 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 and then mapped with DWT over the quantized image. 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 development of this work. Furthermore, Section 4 is about our experimental results. Finally, the conclusion will be in the Section 5.

II. RELATED WORK

In 2006, Chang and Wu proposed an adaptive data-hiding method based on VQ. The Chang–Wu method consists of three procedures: the codeword grouping procedure, the data embedding procedure, and the data extracting procedure. In the grouping procedure, the method iteratively selects an initial codeword with the smallest index as the seeding codeword. Then, it finds out all the closest codeword to the seeding codeword with a given threshold (TH), and merges the codeword's into the same group. The loop continues until all the codeword's are put into some groups. In the data-embedding procedure, the secret data is embedded into the index table. The capacity for embedding secret data depends on the size of the group to which the current encoding codeword belongs. If the group has n codeword's, then the capacity was _log2 n_. Some codeword's are discarded if their group orders are not in the range 0, 2_log 2n_−1. In the extracting procedure, the decoder must restore the same groups described in the embedding procedure, and then extracts the secret bits according to the order of the codeword in the group [11].

C.-C. Chang in 2007, proposed a lossless and reversible steganography scheme which used each block of quantized discrete cosine transformation (DCT) coefficients in JPEG images for embedding secret data. As the need for enhanced security, had led to the development of other algorithms. LSB technique had weak resistance to attacks. So to overcome this shortcoming, researchers found that information should be hide in areas of the image that are less exposed to compression, cropping, and image processing. In the scheme, the two successive zero coefficients of the medium-frequency components of each block were used to hide the secret data. This method results in a high image quality of stego image and successfully achieves reversibility [12].

S. Roy, A. K. Sen, N. Sinha in 2010 proposed a hybrid image compression method based upon two compression technique Vector Quantization (VQ) and Discrete Cosine Transform (DCT). They generated a codebook using DCT matrix and any image can be compressed using this code book. Appropriate codeword's were listed for the selected image and the compressed image had obtained. The Proposed approaches were tested on standard images and their performance was compared with standard VQ method. The Standard images were compressed using both the standard VQ method and proposed method with different block sizes and the PSNR as performance index was obtained for each case for comparison. It was observed that using the proposed image compression method the PSNR is improved for all the images [13].

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, MSE and PSNR 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 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 [14].

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 produced 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[15].

Stuti Goel, Arun Rana & Manpreet Kaurin 2013, had done analysis of LSB, DCT & DWT methods by 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 was implemented in spatial domain in which the payload bits were embedded into the least significant bits of cover image to derive the stego-image whereas DCT & DWT algorithm were implemented in frequency domain in which the stego-image was transformed from spatial domain to the frequency domain and the payload bits were embedded into the frequency components of the cover image. The performance and comparison of these three techniques was evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness. From the results it was concluded that the PSNR of DCT was high as compared to the other two techniques. This showed that the DCT provide best quality of the image. MSE of DWT method was high whereas the Payload is high in LSB method. They also concluded that the DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and it provides maximum security [16].

III. DESIGN AND DEVOLPMENT

Image Steganography includes several techniques of hiding the payload within the cover image. The most popular hiding techniques are Spatial Domain based Steganographic Techniques and Transform 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 viz., Fast Fourier Transform, DCT, Discrete Wavelet Transform (DWT) and Integer Wavelet Transform. In our proposed work spatial domain and frequency domain techniques are used for both encoding and decoding of the images. We used DCT DWT and IDWT 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.

System Flowchart

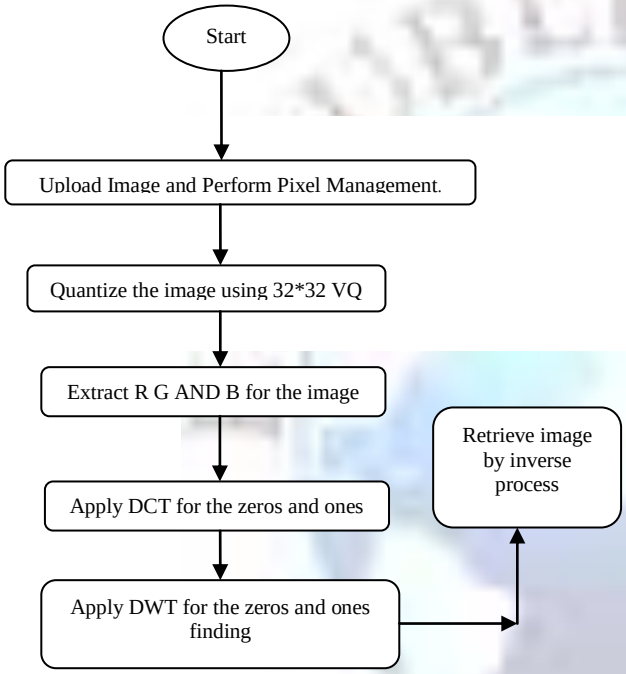

Fig. System flow chart

The proposed method consists 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) Mapping of dwt over the quantized image.
5) Finding out vacant bits using the overlapped image
6) Binarization of the secret message.
7) Embedding the binarized message into quantized image using IDWT.
8) To apply Dequantization in order to get the stego image in spatial domain and compare the stego image and cover image.
9) Evaluate the parameters.

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, DWT 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 Lena.

Our experiments are executed on MATLAB R2010B windows 7, CPU Core i5 with 2 GB of ram, four 512x512-pixel colour images of Lena, penguins, koala 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, i.e. it measures the percentage of the stegno data to the image percentage. PSNR is calculated Equation below:-

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

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

2) Mean Square Error (MSE)

It is defined as the square of error between cover image and stegoimage. 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 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.

4) Computational time

It is the total time consumed for the retrieval of the image which has been embedded into the base image. In our proposed method we had used cover images of Leena, pepper, penguins and koala. The used cover images are given below. Two sizes of image are used one of 256×256 and 512×512 pixel size are used.

Leena(1) Pepper(2) Penguins(3) Koala(4)

Calculated parameters of the Stego-Images (DB)

TABLE 1

Our Method	Image of size 256×256			
	Psnr	MSE	Capacity	Time
Lena	63.26	0.0596849	84198.4	0.25109
pepper	59.0121	0.156189	84198.4	0.18443
koala	61.729	0.0849118	84198.4	0.20623
penguins	59.4397	0.143844	84198.4	0.19012

TABLE 2

Our Method	Image of size 512×512			
	Psnr	MSE	Capacity	Time
Lena	69.3046	0.0149363	336794	0.15436
pepper	65.1157	0.038931	336794	0.16193
koala	67.8408	0.0207865	336794	0.18152
penguins	65.4928	0.0356932	336794	0.19434

CONCLUSION AND FUTURE WORK

In this paper, we implemented the proposed method on four color images namely Lena, pepper, koala and penguins 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. From the work which we have done on 256×256 pixel images and in table 2 on 512×512 and from calculated values it has been found that results are better if image size is increased. It can be concluded that 32×32 vector quantization is a very efficient technique for the image stegnography if it is combined with DCT, DWT & IDWT technique. The results which we have concluded are quite improved from the previous work. The results are quite effective with our method also but in future if someone can try his hands over Neural Networks, it might provide some better results.

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]. "Shailender Gupta, Ankur Goyal, Bharat Bhushan", Information Hiding Using Least Significant Bit Steganography and Cryptography, I.J.Modern Education and Computer Science, 2012, 6, p.27-34.
[4]. A Tutorial Review on Steganography Samir K Bandyopadhyay, Debnath Bhattacharyya ,Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, IC3–2008 UFL & JIITU.
[5]. Robert Krenn, "Steganography and steganalysis".
[6]. Francesco Queirolo, "Steganography in Images".
[7]. 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.
[8]. 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.
[9]. 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.
[10]. 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.
[11]. C. C. Chang and W. C. Wu, "Hiding secret data adaptively in vector quantisation index tables," IEE Proc. Vision, Image Signal Process., vol. 153, no. 5, pp. 589–597, 2006.
[12]. C.C. Chang et al., "Reversible hiding in DCT based compressed images", Information Sciences 177 (2007) 2768–2786.
[13]. Assam University Journal of Science & Technology : Physical Sciences and Technology, Vol. 5 Number II 73-80, 2010 Assam University, Silchar VQ-DCT Based Image Compression: A New Hybrid Approach S. Roy, A. K. Sen, N. Sinha.
[14]. Neha Batra, Pooja Kaushik, "Implementation of Modified 16×16 Quantization Table Steganography on Colour Images, Volume 2, Issue 10, October 2012 ISSN: 2277 128X.
[15]. 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.
[16]. Stuti Goel, Arun Rana & Manpreet Kaur, "A Review of Comparison Techniques of Image Steganography", Global Journal of Computer Science and Technology, (F) Volume XIII, Issue IV Version I, 2013.