Implementation of 16 * 16 Quantization Table Steganography on Gray Scale Images

Hina Anand[1], Kapil Narwal[2], Kartik Mudgal[3]

[1, 2]Manav Rachna College of Engineering, Faridabad, India
[3]University Institute of Engineering & Technology, Rohtak, India

Abstract: ***Steganography is defined as an art of concealed data sharing for communication that prevents the detection of hidden messages. This paper presents a steganographic method based on modification of JPEG quantization table. Modified Discrete Cosine Transform (MDCT) is implemented based on transform domain technique. The proposed work hides the secret message inside an image using Modified Discrete Cosine Transform (MDCT). In this paper, the image is divided into non-overlapping blocks of 16*16 so as to embed secret information. The secret message is hidden inside an image which forms a stego image. The stego image is a combination of secret message and the cover image. Here four grayscale images have been considered and these images have been compared on the basis of three performance parameters such as capacity, PSNR, MSE.***

Keywords: Peak Signal to Noise Ratio, Mean Square Error, Discrete Cosine Transform, Steganography

1. Introduction

Computer networks have become part and parcel in our day to day lives. Securing the network has now become everyone's need either directly or indirectly. Data needs to be secure when it is to be transferred over a network. It can be accomplished through hiding information. Steganography is the technique of invisible communication. The word steganography is derived from Greek words "stegos" meaning cover and "grafia" means writing and when combined together becomes covered writing. The practice of hiding information has a huge history. Information, especially photographs was reduced in size until it was the size of a typed period. Extremely difficult to, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information [4].

Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography hides the secret message within cover files (i.e. images, music and video files). Therefore, confidentiality and data integrity are needed to protect against unauthorized user. Cryptography and steganography are two popular methods available to provide security. Cryptography is created as a technique to provide security to information. The differences between two methods are that steganography deals with preventing the existence of communication whereas cryptography prevents unauthorized party from discovering contents of communication. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Steganography is defined as practice of disguising or hiding the existence of message [2]. All digital file formats can be used for steganography, but only those formats are useful that have high degree of redundancy. There are different categories of file format used for steganography. They are: text, images, audio/video and protocol. In comparison to all the above categories, images are the most popular cover objects for steganography. In image steganography, information is hidden exclusively in images. An image is a collection of numbers and this numeric representation forms a grid and individual points are referred to as pixels. Most images consist of rectangular map of pixel and each pixel is displayed horizontally row by row. Grayscale images use 8 bits for each pixel and display 256 different colors. Sometimes, when working with images of large size, images become too large to transmit over a channel [2]. In order to display, techniques are used so as to reduce size of the file. This process is referred to as compression. In images there are two types of compression techniques: lossy and lossless. Lossy compression creates smaller files by removing excess image from original image. An image format that uses this compression technique is JPEG [3]. Lossless compression never removes data in mathematical notation. The file format that uses this technique is GIF. Image steganography techniques can be divided into two groups: Image domain and Transform domain.

The paper is organized in the following sections. Section II reviews the related work on JPEG steganographic methods. Section III describes the concept of image steganography. Section IV describes our proposed steganographic model and discusses the algorithms used for embedding and extracting process. Section V describes the evaluation parameters. Section VI discusses the results evaluated. Finally, the conclusion is presented in section V.

2. Related Work

Hiding the data in text had been earlier method, but nowadays images are the most popular cover objects. In the domain of digital images, different image file formats are used. Different carrier file formats are used, but digital images are the most popular because of their frequency on Internet. There exist a large variety of steganographic techniques for hiding secret information in images. In the related work, the most common method which is used to hide the message involve the usage of LSB developed by Chandramouli et.al [1] by applying filtering, masking and transformation on the cover media. Hiding data is the process of embedding information into digital content without causing perceptual degradation. Steganography

based on JPEG applies 2-DCT transform. The process starts by dividing the cover image into blocks of 8*8 pixels, performing DCT and finally using standard 8*8 quantization tables, a well known steganographic tool Jsteg, embeds the secret data in LSB. Chang et.al [2] proposed high capacity steganography with modified 8*8 quantization table.

Different techniques have been developed for transformation by various researchers. DCT has been adopted in image compression standards. Akhil Khare et al [8] proposed a framework for hiding large volumes of data in images while incurring minimal perceptual degradation. The techniques involved 2D discrete cosine transform (DCT) of non-overlapping 8*8 blocks, followed by embedding in selected DCT coefficients. K B Shiva Kumar et al [7] proposed a Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT). The cover image was segmented into 8*8 blocks and DCT was applied on each block. The numbers of payload MSB bits were embedded into DCT coefficients of cover image based on DCT coefficients. Based on Chang's quantization paper Jiang Cuiling et.al [3] proposed a method of dividing the cover image into 16*16 pixels which resulted in better quality image and higher capacity. In our proposed method, we are going to divide the cover image into non-overlapping blocks of 16*16 pixels and use large quantization table so as to improve the embedding capacity in gray-scale images.

3. Image Steganography

Images have been the most popular cover images for use in steganography. There are two kinds of image steganographic techniques. They are spatial and frequency domain techniques. The schemes of first kind directly embed the secret data within the pixels of the cover image such as Least Significant Bit (LSB). The schemes of the second kind embed the secret data within the cover image that has been transformed such as Discrete Cosine Transform (DCT). The DCT coefficients of transformed cover image are quantized, and these coefficients are then modified according to the secret data [1]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [8]. Steganography in the transform domain involves the manipulation of algorithms and image transforms. These methods are used to hide the messages in more significant areas of the image, making it more robust. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression. Almost all digital file formats can be used for steganography, but the formats that are most suitable are those with high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display [4]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files comply with this requirement. One of the most popular image formats that are widely used on Internet and World Wide Web (WWW) is JPEG. Among all the file formats, the JPEG file format is the most popular image file format on the Internet, because of the small size of the images. JPEG compression provides large compression ratio and maintains high image quality [9].

4. Proposed Work

Our proposed work includes two procedures- embedding procedure and extracting procedure.

4.1 Embedding procedure

In embedding procedure, first the cover image is divided into non-overlapping blocks of 16*16. The secret data is embedded into the quantized DCT coefficients after quantization [7]. The steps are as follows:

1. A grayscale image is taken and a message is generated for hiding inside the image.
2. Secret message is encrypted and converted to binary format.
3. Then, the cover image is segmented into non-overlapping blocks of 16*16. Then they are further transformed into DCT coefficients in transform domain.
4. Discrete Cosine Transform converts each block into DCT coefficient matrix.
5. A quantization table is selected and is DCT coefficients are quantized with the quantization table using the formula as given below:

$$\text{Round}\left(\frac{\text{DCT } 8 \times 8 \text{ block}}{\text{Quantization Table}}\right) = \textit{Sparse Matrix} \quad (1)$$

The ideal Discrete Cosine Transform is of the form as shown below:

$$F(u,v) = (1/4)[C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) \cos\left(\frac{(2x+1)u\pi}{16}\right)\cos\left(\frac{(2y+1)v\pi}{16}\right)],$$

$$\text{where} \quad C(u), C(v) = \begin{cases} 1/\sqrt{2} & \text{for } u, v = 0, \\ 1 & \text{for all other values of } u, v. \end{cases} \quad (2)$$

6. Run-length encoding is applied on the calculated quantized coefficients so as to achieve the compressed image. Figure below shows the 16*16 quantization table used in our method.

$$\begin{bmatrix}
16 & 8 & 7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
7 & 7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 30 \\
7 & 6 & 6 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 30 & 28 \\
6 & 8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 32 & 35 & 29 \\
8 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 32 & 35 & 32 & 28 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 40 & 42 & 40 & 35 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 44 & 42 & 40 & 35 & 31 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 35 & 44 & 44 & 50 & 53 & 52 & 45 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 31 & 34 & 44 & 55 & 53 & 52 & 45 & 39 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 31 & 34 & 40 & 41 & 47 & 52 & 45 & 52 & 50 \\
1 & 1 & 1 & 1 & 1 & 1 & 30 & 32 & 36 & 41 & 47 & 52 & 54 & 57 & 50 & 46 \\
1 & 1 & 1 & 1 & 1 & 36 & 32 & 36 & 44 & 47 & 52 & 57 & 60 & 60 & 55 & 50 \\
1 & 1 & 1 & 1 & 36 & 39 & 42 & 44 & 48 & 52 & 57 & 61 & 60 & 60 & 55 & 51 \\
1 & 1 & 1 & 39 & 42 & 47 & 48 & 46 & 59 & 57 & 56 & 55 & 52 & 51 & 54 & 51 \\
1 & 1 & 41 & 46 & 47 & 48 & 48 & 49 & 53 & 56 & 53 & 50 & 51 & 52 & 51 & 50 \\
1 & 43 & 47 & 47 & 48 & 48 & 49 & 57 & 57 & 56 & 50 & 52 & 52 & 51 & 50 & 50
\end{bmatrix}$$

Figure 1: 16*16 Quantization Table

4.2 Extracting Procedure

In extracting procedure, the secret message is retrieved by applying dequantization on 16*16 table. Then, dequantized image is converted to spatial domain by implementing IDCT (Inverse Discrete Cosine Transform). As a result, stego image is obtained. The steps are as follows:

1. Run-length decoding is performed on the compressed image.
2. Dequantization using 16*16 quantization table is achieved.
3. Then, dequantized JPEG image is converted to spatial domain by implementing IDCT (Inverse Discrete Cosine Transform).
4. Then, JPEG image is segmented into 16*16 blocks.
5. As a result, stego image is obtained.

5. Evaluation Parameters

There are various evaluation parameters that are being used by various researchers like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Hiding Capacity. All of them are discussed below one by one.

5.1 Mean Square Error (MSE)

It is defined as the square of error between the cover image and the stego image. The distortion in the image can be measured using MSE and is calculated using equation (3) below:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - \bar{X}_{ij}\right)^2 \quad (3)$$

where X_{ij} = pixel value of cover image

X_{ij}' = pixel value of stego image

N = size of image

5.2 Peak Signal-to-Noise Ratio (PSNR)

It is defined as the measure of quality of the image by comparing the cover image with the stego image. In other words, we can say that it measures the statistical difference between the cover and the stego image [6]. It is calculated using equation (4) below:

$$PSNR = 10x\log\frac{255^2}{MSE}db \quad (4)$$

5.3 Hiding Capacity

It is defined as the size of the data in the cover image that can be modified without disintegrating the integrity of the cover image [5]. Capacity is represented by bits per pixel (bpp) whereas Maximum Hiding Capacity (MHC) is measured in terms of percentage.

6. Results and Discussions

Four grayscale images are used as test images. These cover images are Lena (1), Pepper (2), Sun (3), Girl (4).

Lena (1) **Pepper (2)**

Sun (3) **Girl (4)**

Figure 2: Test images

Table 1: Comparison of Hiding Capacity, MSE and PSNR

Image	*Pixels*	*Hiding Capacity*	*MSE*	*PSNR*
1.Lena	256*256	69632	0.0133	66.883
	512*512	278528	0.0251	64.1282
2.Pepper	256*256	69632	0.0931	56.971
	512*512	278528	0.025	62.2132
3.Sun	256*256	6932	0.1771	55.6473
	512*512	278528	0.0324	63.018
4.Girl	256*256	69632	0.0944	58.3766
	512*512	278528	0.024	64.3199

The steganographic methods were used and were coded in MATLAB R2011b and run on a Pentium P4 with 1GB RAM under Windows operating system. Table 1 below shows the comparison of Hiding Capacity, MSE and PSNR.

References

[1] Chandramouli, R. and Memon N. (2001). Analysis of LSB Based Image Steganography Techniques. In Proceedings of IEEE ICIP.

[2] Chang, C.C. Chen, T.S. and Chung, L.Z. (2002). A steganographic method based upon JPEG and quantization table modification. Information Sciences, 141, 123-138.

[3] Jiang Cuiling, Pang Yilin, Guo Lun, Jing Bing, Gong Xiangyu. (2011). A High Capacity Steganographic Method Based on Quantization Table Modification. Springer-Verlag Berlin Heidelberg, 16(3), 223-227.

[4] Mahajan, S. Singh, A. (2012). A Review of Methods and Approach for Secure Steganography. International Journal of Advanced Research in Computer Science and Software Engineering. 2(10), 67-70.

[5] Yadav, R. (2011). Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters. International Journal of Computer Technology and Application. 2(6), 1867-1870.

[6] Yadav, R. (2011). Analysis of Various Image Steganography Techniques Based Upon PSNR Metric. International Journal of P2P Network Trends and Technology. 1(2).

[7] Kumar, K. Raja, K. Chhotaray, R. and Pattanaik, S. (2010). Bit Length Replacement Steganography Based on DCT Coefficients. International Journal of Engineering Science and Technology. 2(8), 3561-3570.

[8] Khare, A. Kumari, M. and Khare, P. (2010).Efficient Algorithm for Digital Image Steganography. Journal of Information, Knowledge and Research in Computer Science and Applications. 1(1).

[9] Jain, A.K., Fundamentals of Digital Image Processing, Prentice-Hall, 1989.

Author Profile

Hina Anand received B.Tech Degree in Computer Engineering from Maharshi Dayanand University, Rohtak in 2010. She just completed her M.Tech in Computer Engineering from Manav Rachna College of Engineering, Faridabad.

Kapil Narwal received B.Tech and M.Tech Degree in Mechanical Engineering from Maharshi Dayanand University, Rohtak. He is currently now Assistant Professor in Manav Rachna College of Engineering, Faridabad.

Kartik Mudgal received B.tech Degree in Computer Science from University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak.