Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Steganography Using Various Quantization Techniques: A Review

Tara Bansal, Ruchika Lamba
Department of Electrical & Instrumentation Engineering
Thapar University, Patiala, India

Abstract: ***Steganography is the art of passing information in a manner that the very existence of the message is unknown. 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. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. This paper presents a review on various quantization tables used for Steganography. Firstly, the concept of steganography is introduced and then different quantization tables, such as 8x8 and 16x16, both on gray scale and colored images are reviewed***

Key Words: Steganography, Quantization, JPEG

1. Introduction

Steganography is the art of covered or hidden writing [1]. The purpose of steganography is covert communication to hide a message from a third party. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is that the output of cryptography is scrambled so that it can draw attention but the output of steganography operation is not apparently visible, so both techniques have difference in the appearance in their processed outputs. Steganography and Cryptography are great partners in spite of functional difference. It is common practice to use cryptography with steganography [2]. Its ancient origins can be traced back to 440 BC. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [3]. The majority of today's steganographic systems uses multimedia objects like image, audio, video etc. as cover media because people often transmit digital pictures over email and other Internet communication. Secret message within other innocuous-looking cover files (i.e. images, music and video files) so that it cannot be observed. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness

1.1 Steganography Mechanism

Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence. Block diagram of steganography mechanism is shown in Figure 1.

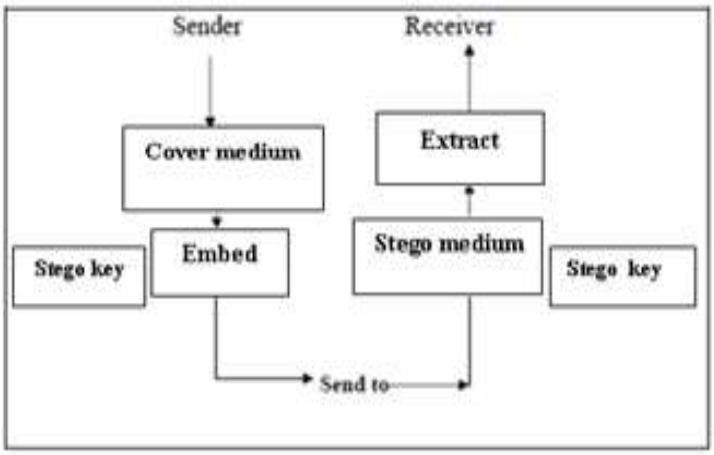

Figure 1.1 Block Diagram of Steganography Mechanism [4]

Here a secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process. The proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

1.2 Types of Steganography

In modern approach, depending on the nature of cover object, steganography can be divided into five types:

1.2.1 Text Steganography: Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters). It includes line-shift coding, word-shift coding and feature coding [5].

1.2.2 Image Steganography: Images are the most popular cover objects used for steganography. . In the domain of digital images many different file formats exist and for these file formats different algorithms exist. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

1.2.3 Audio Steganography: In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

1.2.4 Video Steganography: Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

1.2.5 Protocol Steganography: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. There are covert channels in the layers of the OSI network model where steganography can be used.

1.3 Uses of Steganography

The three most popular and researched uses for steganography in an open systems environment are covert channels, embedded data and digital watermarking [6]. Covert channels can be very useful for any secure communications needs over open systems such as the Internet. By embedding the hidden data into the cover message and sending it, you can gain a sense of security by the fact that no one knows you have sent more than a harmless message other than the intended recipients Digital watermarking is very important in the detection and prosecution of software pirates/digital thieves. Steganography is used by some modern printers, including HP and Xerox brand color laser printers.

2. Quantization

Quantization is the procedure of constraining something from a relatively large or continuous set of values (such as the real numbers) to a relatively small discrete set (such as the integers. The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform but using only real numbers. There are eight standard DCT variants, of which four are common. The most common variant of discrete cosine transform is the type-II DCT, which is often called simply "the DCT"; its inverse, the type-III DCT, is correspondingly often called simply "the inverse DCT" or "the IDCT". Two related transforms are the discrete sine transforms (DST), which is equivalent to a DFT of real and odd functions, and the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data.

2.1 Bit Length Replacement Steganography Based on DCT Coefficients (BLSDCT)

In BLSSDCT steganography the cover image is segmented into 8*8 blocks and DCT is applied on each block. The numbers of payload MSB bits are embedded into DCT coefficients of the cover image based on the values of DCT coefficients. The algorithms used in this technique are embedding algorithm and the retrieval algorithm [7].

2.1.1Embedding algorithm:

Inputs: Cover image and Payload

Output: Stego image

- A cover image of any size and format is considered and is converted to gray scale.
- Apply pixel management to the cover image, to avoid overflow and underflow
- Segmentation of cover image into 8*8 blocks and are transformed into DCT domain
- The number of bits *L* of each DCT coefficient of cover image to be replaced by the payload MSB bits using coherent bit length
- The stego image obtained in the DCT domain is converted into the spatial domain using IDCT.

2.1.2 Retrieval algorithm

Input: Stego image

Output: Retrieved Payload

- The stego image is segmented into 8*8 blocks.
- The 8*8 blocks are transformed into frequency domain using DCT.
- The payload length *L* for each DCT coefficient is calculated similar to the procedure adapted in the embedding technique.
- Extract *L* bits from each DCT coefficients.
- The payload is constructed using *L* number of bits.

The most powerful and quantization technique used for the image compression is vector quantization(VQ).The vector quantization algorithms for reducing the transmission bit rate or storage have been extensively investigated for speech and image signals. Image vector quantization (VQ) includes four stages: vector formation, Training set selection,

codebook generation and quantization. The first step is to divide the input image into set of vectors. The Subset of vectors in the set is later chosen as a training sequence. The codebook of code words is obtained by an iterative clustering algorithm. Finally, in quantizing an input vector, closest code words in the codebook is determined and corresponding label of this code word is transmitted. In this process, data compression is achieved because address transmission requires fewer bits than transmitting vector itself. The concept of data quantization is extended from scalar to vector data of arbitrary dimension. Instead of output levels, vector quantization employs a set of representation vectors (for one dimensional case) or matrices (for two dimensional cases). Set is defined as "codebook" and entries as "code words". Vector quantization has been found to be an efficient coding technique due to its inherent ability to exploit the high correlation between the neighboring pixels [3].

3. Steganographic Method Based On Jpeg Quantization

JPEG technique divides the input image into non-overlapping blocks of 8x8 pixels and uses the DCT transformation. For each quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient are modified to embed two secret bits. Using gray-level cover images, we transformed (DCT) non-overlapping blocks of 16x16 pixels instead of non-overlapping blocks of 8x8 pixels. The transformed DCT coefficients were quantized by a modified 16x16 quantization table. Then, we embedded the secret data within the middle frequency coefficients

3.1 Quantization Table

The JPEG standard uses 8x8 quantization tables, but it does not specify default or standard values for quantization tables. Table I shows the standard 8x8 blocks luminance quantization table in JPEG.

Table I. The standard (8×8 blocks) luminance quantization table in JPEG [8]

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Dividing this quantization (Table I) by 2, we get a new quantization table (Table II).

Table II. The scaled quantization table (scale factor = 2) [8]

8	6	5	8	12	20	26	31
6	6	7	10	13	29	30	28
7	7	8	12	20	29	35	28
7	9	11	15	26	44	40	31
9	11	19	28	34	55	52	39
12	18	28	32	41	52	57	46
25	32	39	44	52	61	60	51
36	46	48	49	56	50	52	50

Using this new quantization table generates reconstructed images almost identical to the source image. The modified version of (Table II), has been used within Chang et al. method. 8x8 quantization tables apart, there are no samples for larger quantization tables in the JPEG standard.

Table III. The modified quantization table [8]

8	6	5	8	1	1	1	1
6	6	7	1	1	1	1	28
7	7	1	1	1	1	35	28
7	1	1	1	1	44	40	31
1	1	1	1	34	55	52	39
1	1	1	32	41	52	57	46
1	1	39	44	52	61	60	51
1	46	48	49	56	50	52	50

Consequently, we produced a 16x16 quantization table (Table IV) by simulating and stretching the scaled quantization table (Table II)

Table IV Our suggested 16x16 quantization table [8]

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	49	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

4. Steganography On Colour Images Using 16x16 Quantization

It is a novel steganographic method based on the JPEG quantization table modification. Instead of dividing cover image into 8×8 blocks, the cover image is divided into non-overlapping blocks of 16×16 pixels to embed secret information.

4.1 Algorithms

The different algorithms used for this method are embedding algorithm and retrieval algorithm.

4.1.1Embedding algorithm

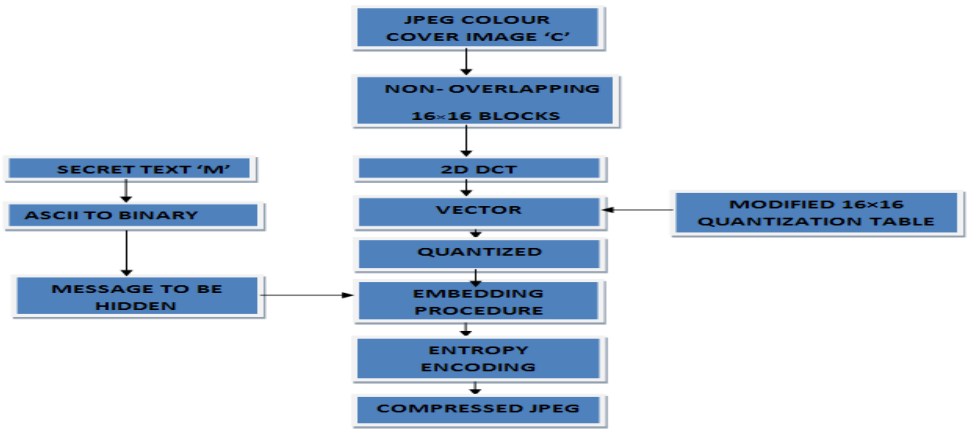

Figure 4.1.1 Embedding Procedure [9]

4.1.2 Retrieval algorithm

The secret message is retrieved for the stego image by the adaptive reverse procedure of embedding and is shown in the figure 4.1.2.

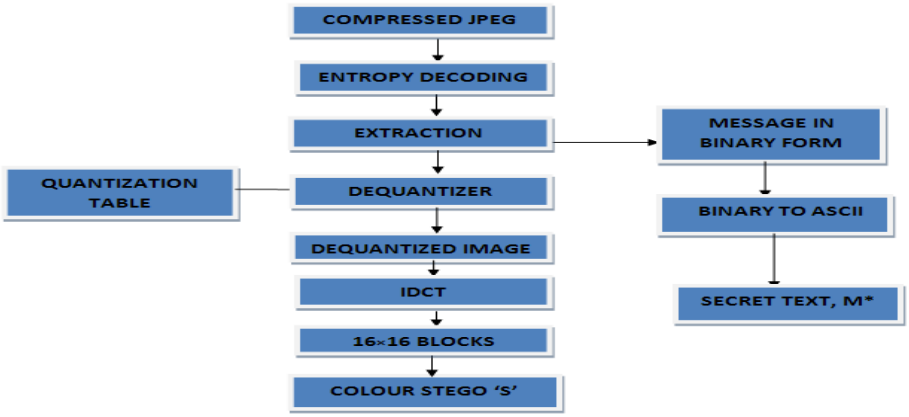

Figure 4.1.2 Extracting Procedure [9]

This method shows high performance with regard to embedding rate and PSNR of stego image. Furthermore, the produced stego-images are almost identical to the original cover images.

V. Conclusion

Steganography aims to hide the very existence of communication by embedding messages within other cover objects. Both colour and gray scale images can be used as cover images because some steganography methods use colour JPEG images as test images while others use gray scale images. We have reviewed different quantization methods in this paper and concluded that various parameters like PSNR, MSE, Capacity increases as number of modified coefficients increases. It also shows that steganography using 16x16 quantization tables gives improved results than 8x8 quantization tables. In future, our proposed work is performing steganography on color images using 32x32 Quantization on standard test images and give improved results for various parameters namely, PSNR, MSE, Hiding Capacity.

References:

[1] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[2] "Steganography and Steganalysis: Different Approaches", Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal.

[3] "A Tutorial Review on Steganography", Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das.

[4] "Video Steganography by LSB Substitution Using Different Polynomial Equations", A. Swathi, Dr. S.A.K Jilani, International Journal of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

[5] "An overview of image steganography", T Morkel, J.H.P. Eloff, M.S.Olivier.

[6] "A Detailed look *at Steganographic* Techniques and their use in Open System Environment", SANS Institute.

[7] "Bit Length Replacement Steganography Based on DCT Coefficients", 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

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

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

