International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN : 2278-800X, www.ijerd.com
Volume 5, Issue 5 (December 2012), PP. 42-47

Quantization Table Based Steganography System

Parmanand Dewangan[1], Monisha Sharma[2], Swagota Bera[3]
[1]M.E (Student), Electronics & telecommunication, CSVTU, SSCET, Bhilai, India
[2]Associate Professor, Electronics & Telecommunication, CSVTU, SSCET, Bhilai, India
[3]Reader, Electronics & Telecommunication, CSVTU, SSIET, Bhilai, India

Abstract:- Steganography is an important area of research in recent years involving a number of applications. Steganography is the process of hiding one file inside another such that others can neither identify the meaning of the embedded object, nor even recognize its existence. One of the most Common methods of implementation is Least Significant Bit (LSB) Insertion in which the least significant bit of every byte is altered to form the bit-string representing the embedded file. Altering the LSB will only cause minor changes in colour, and thus is usually not noticeable to the human eye *[4]*. The two most important aspects of any image based steganographic system are the imperceptibility and the capacity of the stego image. It is desired to maximize the amount of hidden information (embedding rate) while preserving security against detection by unauthorized parties. A steganographic system is perfectly secure when the statistics of the cover data and the stego data are identical, which means that the relative entropy between the cover data and the stego data is zero. For image data, another constraint is that the stego data must look like a "typical image." This paper evaluates the performance and efficiency of using optimized quantization tables instead of default JPEG tables within JPEG steganography. We found that using optimized tables significantly improves the quality of stego-images. Our experimental results show that the proposed approach can provide a higher information-hiding capacity than the other methods tested. Furthermore, the quality of the produced stego-images is better than that of other methods which use the default tables *[2]*.

Keywords:- LSB Insertion, JPEG, Steganography, Imperceptibility, Entropy, Optimized, Quantization table.

I. INTRODUCTION

In the present electronic communication scenario, data security is one of the major challenges. After the World War II, the need for a secure and robust communication between the communicating entities has increased due to the fear of terrorism. Over the last three decades, people have sought ways to protect sensitive information against attack to make sure it is not received by unintended recipients. The publishers of digital audio and video are worried of their works being corrupted by illegal copying or redistribution, hence it is of primary importance to protect information *[6]*. Steganography is derived from the Greek word steganographic which means covert writing. It is the science of embedding information into cover objects such as images that will escape detection and retrieved with minimum distortion at the destination. The resultant image object obtained after embedding information into the cover image is called as stego object *[1]*.

Message transmissions over the Internet still have data security problems. Therefore, secure and secret communication methods are needed. Cryptography is the method to hide secret data by scrambling so that it is unreadable, however it does not assure security and robustness as the hacker can obviously guess that there is a confidential message passing on from the source to the destination. Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it, but the most important factors to be concern in Steganography are:

- Size of information to be hidded i.e. capacity of cover media.
- Imperceptibility i.e. quality of cover media *[5]*.

Some of the well-known steganography methods are the following: LSB, masking and filtering and transform technique. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Most Significant Bits (MSB) of the image to be hidden without destroying the statistical property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In

masking and filtering techniques two signals are embedded into each other in such a manner that only one of the signals is perceptible to the human eye. This is mainly used in watermarking techniques. In the transform based method, the spatial domain is transformed to frequency domain using DCT, Fast Fourier Transforms (FFT), and Wavelets etc. *[1]*.

In JPEG compression, the image is divided into disjoint blocks of 8x8 pixels, a 2-dimensional DCT is applied to each block, and then the DCT coefficients of these blocks are quantized and coded. Most of the steganographic techniques used for JPEG images adopt the standard JPEG compression. The cover image is divided into non-overlapping blocks of 8x8 pixels in order to perform DCT and provide compressed images *[2]*. Although the JPEG standard uses 8x8 quantization tables, it does not specify default or standard values for quantization tables. However, the JPEG standard provides a quantization tables for its YCbCr component separately. Since this quantization table is widely used, it will be called the JPEG default quantization table.

Table I the default JPEG quantization table (DQT)

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

II. RELATED WORK

The proposed LSB based algorithm in which the quality of the retrieved image is poor. To optimize the steganographic method of [1] in terms of capacity and stego-image quality transform domain is used. Furthermore increasing the capacity while maintaining the imperceptibility is still a challenge. However, many novel embedding techniques have been suggested in order to enhance the security and increase the capacity of steganographic methods.

Since the quantization table is not part of the JPEG standard, users are allowed to design or redefine the quantization table to control the quality of the reconstructed image. A DCT co-efficient algorithm in which MSBs of hidden image are embedded into insignificant DCT coefficients of the cover image is presented in *[6]*. To obtain DC coefficients quantization table is used which improves the Steganographic parameters. The usage, advantages, and limits of existing steganography techniques are analysed.

III. METHODOLOGY

In this section, we describe the Least Significant Bit Algorithm, Discrete Cosine Transformation to obtain stego-image. Stego-image is the combination of cover image and hidden document. DCT is used to convert stego-image in spatial domain into stego-image in frequency domain for enhanced security. The reverse process is carried out at the receiver end, where the hidden document is retrieved from the encoded stego-image using the inverse transform techniques like inverse DCT (IDCT) and inverse process of LSB Technique *[1]*.

A. Least significant bit (LSB) embedding

A simple LSB substitution, which hides secret data directly into LSBs, is easily implemented. The procedure for such technique is to convert the desired hidden message into binary form and then encrypt each digit into a least significant bit of the cover image. For example, 11111111 is an 8-bit binary number. The rightmost bit is called the LSB because changing it has the least effect on the value of the number. The idea is that the LSB of every byte can be replaced with little change to the overall file.

For 24-bit image

Pixel: - (00100111 11101001 11001000)

Insert**:**--- 101**:**

(0010011 11101000 11001001)

Red Green Blue

B. Discrete cosine transform

A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. The DCT is used in JPEG image compression and secure data hidding. There, the two-dimensional DCT-II of N×N blocks is computed and the results are quantized and hidding technique is applied. In this case, N is typically 8 and the DCT-II formula is applied to each row and column of the block. The result is an 8 × 8 transform coefficient array in which the (0,0) element (top-left) is the DC (zero-frequency) component and entries with increasing vertical and horizontal index values represent higher vertical and horizontal spatial frequencies. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and output data are shifted by half a sample *[11]*.

In image processing with a JPEG system, it is possible to control the image quality and compression ratio by controlling values in quantization table *[2]*. Therefore, it is useful to find a quantization table with better image quality than obtained by the JPEG default tables. For that process the quantization table was partitioned into four bands by frequency. Subsequently, each value in each band was changed and then the quality of image was examined. As a result, it was found that the DC coefficient has an important effect on the image quality while the higher frequency coefficients have only a secondary importance.

Table II the modified quantization table (MQT)

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

.

As the modified Quantization table provides importance of JPEG compression system, now we are trying to investigate and evaluate the effects of using optimized and modified quantization tables on JPEG steganography. The optimization strategy proposed by Monro and Sherlock are represented by a three parameter model as following:

For 8x8 blocks: $Q_{xy} = A+DZ^F$

Where x and y are the DCT coefficient indices, Z=x+y is the Manhattan distance of a coefficient from (0,0), and A, D, and F are three model parameters;

$A=5.43+2.15C_R$

$D = O.O969 - 0.0565C_R + 0.00749\ C^2_R$

$F=1.83$

Table III the optimized and modified quantization table (OMQT)

8	8	8	9	1	1	1	1
8	8	9	1	1	1	1	14
8	9	1	1	1	1	14	15
9	1	1	1	1	14	15	16
1	1	1	1	14	15	16	18
1	1	1	14	15	16	18	20
1	1	14	15	16	18	20	22
1	14	15	16	18	20	22	23

IV. THE EMBEDDING AND EXTRACTING PROCEDURES

Step I: Take a cover image

Step II: Preprocessing of input image like resizing, data format and converting into 8x8 blocks.
Step III: Apply DCT to the each blocks of cover image.
Step IV: Now apply Quantization table to obtain DC coefficients.
Step V: Now apply LSB replacement technique. The obtain image is Stego image.
Step VI: Now send this Stego image to receiver side.
Step VII: Now again convert stego image into 8x8 blocks and apply DCT and Quantization table for DC coefficients.
Step VIII: Apply reverse LSB algorithm to extract hide document from the cover image.

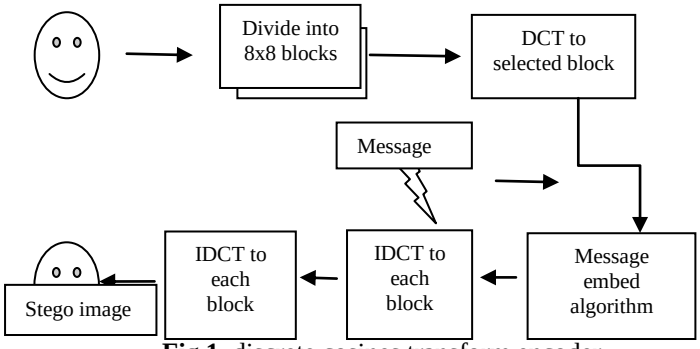


Fig.1. discrete cosines transform encoder

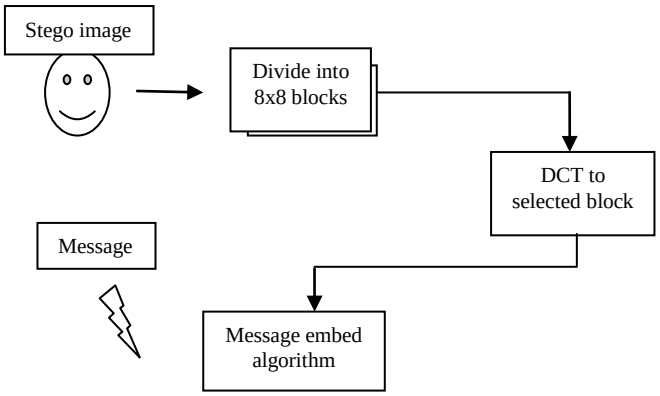


Fig.2. discrete cosine transforms decoder

V. RESULT

In order to evaluate the quality of images some parameters is necessary. Consequently, most researchers use Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) criteria to measure the quality of image coding and compression *[11]*. The Mean Square error (MSE), PSNR and Maximum difference (MD) is calculated by the following equations:

$$MSE = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - \overline{X_{ij}})^2 \quad (1)$$

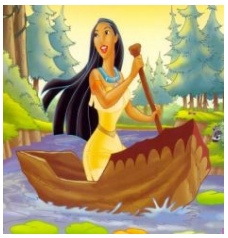
$$PSNR = 10.\log_{10}\frac{I^2}{MSE}\,db \quad (2)$$

$$MD = Max(|(X_{i,j} - \overline{X_{i,j}})|) \quad (3)$$

X_{ij}: The pixel values of the cover image.

$\overline{X_{ij}}$: The pixel values of the stego image


cute.jpg


girl.jpg


bird.jpg


dish.jpg

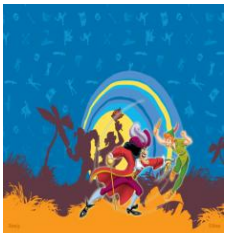

cartoon.jpg

Table IV Parameters comparision of steganographic system

S.No	Name of image	DQT			MQT			OMQT			Capacity (Bits)
		MSE	PSNR	MD	MSE	PSNR	MD	MSE	PSNR	MD	
1	cute	11.922	37.367	169	2.719	43.786	87	0.407	52.034	32	38400
2	girl	11.982	37.3452	122	2.729	43.769	72	0.447	51.618	27	26288
3	bird	8.669	38.751	167	2.382	44.359	79	0.347	52.716	29	87040
4	dish	16.092	36.064	169	3.888	42.233	82	0.606	50.301	28	38400
5	cartoon	8.956	38.609	191	2.140	44.825	89	0.307	53.259	34	38400

VI. CONCLUSIONS

In this paper Steganography, image hiding is done in frequency domain using the LSB substitution technique. The stego images are obtained after hiding secret image and different parameters of stego image are calculated. It is find that PSNR, MSE, Maximum difference and hidding capacity of the cover image and quality of stego image is improved by the use of Optimized and modified Quantization table compare to default table. Hence Pixel value difference between cover and stego images is decrement by using OMQT, so maximum secret data will hidded on cover images further hiding capacity will improved.

In future it is also possible to obtain a more optimized and modified Quantization table which provides better quality and improve Steganographic parameters. Also hiding technique will change in place of LSB to modified parameters.

ACKNOWLEDGMENT

The pleasure, the achievement, the glory, the satisfaction and the construction of my paper cannot be thought of without the few, who apart from their regular schedule spared their valuable time. A person contributed either directly or indirectly in shaping and achieving the desired outcome. The gratitude, I owe a lot, to Monisha Sharma Madam, at this stage, is that without their guidance and help, smooth sailing in this journey of paper preparation would have been extremely difficult. Through their timely advice, constructive criticism and supervision they was a real source of inspiration for me.

The foremost person who comes into my mind to express my deep sense of gratitude is Swagota Bera Madam She was there to help me out through the thick and thin of this paper I also very thankful IJERD LaTeX which provide me platform to present my ideas and share to a lot of peoples.

REFERENCES

[1]. Parmanand Dewangan, Umashanker Dewangan, Monisha Sharma, Swagota Bera, "Image hiding in frequency domain," National level technical paper presentation, 'Technologia', MPCCET, Bhilai, 10th - 11th March, 2011.

[2]. Adel Almohammad, Gheorghita Ghinea, Robert M. Hierons, "JPEG steganography: a performance Evaluation of quantization tables," International Conference on Advanced Information Networking and Applications, 2009.

[3]. Jan, Joachim J. Eggers and R. B¨aum Bernd Girod, "A Communications Approach to Image Steganography," Proceedings of SPIE Vol. 4675 Security and Watermarking of Multimedia Contents IV San Jose, Ca, 2002.

[4]. Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Colour Images," World Academy of Science, Engineering and Technology 50, 2009.

[5]. August, Adel Almohammad, "Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility," Department of Information Systems and Computing Brunel University, 2010.

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

[7]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," School of Computing and Intelligent Systems, Faculty of Computing and Engineering University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, United Kingdom, 2009.

[8]. Husrev T. Sencar, Mahalingam Ramkumar, Ali N. Akansu, "An analysis of Quantization based Embedding detection techniques," 0-7803-8484-9/04/$20.00 ©2004 IEEE.

[9]. T. Pevny and J. Fridrich, "Determining the stego algorithm for JPEG images," The Institution of Engineering and Technology IEE Proceedings online no. 20055147, 2006.

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

[11]. http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.