IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. V (Jan – Feb. 2015), PP 68-74
www.iosrjournals.org

DCT based Steganographic Evaluation parameter analysis in Frequency domain by using modified JPEG luminance Quantization Table

Sourish Mitra[1], Moloy Dhar[2], Ankur Mondal[3], Nirupam Saha[4], Rafiqul Islam[5]
[1](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)
[2](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)
[3](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)
[4](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)
[5](Department of Computer Science & Engineering, Gurunanak Institute of Technology, India)

Abstract : *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. In this paper we want to increase the capacity and performance of DCT based steganography by using modified JPEG quantization table embedding technique in frequency domain. Our experimental results show that the proposed method will provide a better result in terms of some evaluation criteria named Peak Signal to noise ratio, square of error between cover & stego image, maximum no of bits that can be embedded in a cover image with a negligible probability of detection by an adversary of steganography system. Our proposed method shows that after modification of frequency values in default JPEG quantization table we can be able to increase the image quality by increasing the value of Peak signal to noise ratio, capacity and also by decreasing mean square error of embedded image. So that's why when we try to extract hidden data from stego image in receiving end we just get almost exact hidden data with less error possibilities. In our proposed method we first create modified default (8x8) quantization table from default 8X8 traditional JPEG quantization table and then by using the table we can also try to modify embedding as well as extracting algorithm in frequency domain steganography. It has been found that capacity which is the amount of information embedding in color images increases as the number of modified quantized DCT coefficients increases. So more data can be embedded in this innovative approach.*

Keywords: *DCT coefficient, frequency domain, mean square error, peak signal to noise ratio, Quantization table*

I. Introduction

Steganography is derived from the Greek word steganographic which means cover 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. Steganography is the art of concealing information in ways that prevent the detection of hidden messages. Steganography includes an array of secret communication methods that hide the message from being seen or discovered. Three different aspects in information-hiding systems contend with each other: capacity, security, and robustness. If a message is encrypted and hidden with a Steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected. The resultant image object obtained after embedding information into the cover image is called as stego object .But two most important aspects how much data is hidden in cover image and what is the quality of stego image. Diagram of the image based steganography is given below. Steganography data hiding methods are mainly in three types.(a) LSB, (b)masking and filtering and (c) 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. In the transform based method, the spatial domain is transformed to frequency domain using DCT. Data hiding methods for images can be categorized into two categories. They are spatial-domain methods and frequency-domain ones. In the spatial domain [1,2], the secret messages are embedded in the image pixels directly. In the frequency-domain [2, 3], however, the secret image is first transformed to frequency-domain, and then the messages are embedded in the transformed coefficients. Discrete cosine transformer (DCT) is a widely used tool for frequency transformation. There is a JPEG hiding-tool called Jpeg–Jsteg [4]. The main drawback of Jpeg–Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coefficients are almost all zero and cannot hide messages [5]. In our proposed method we just try to increase the capacity using modified quantization table.

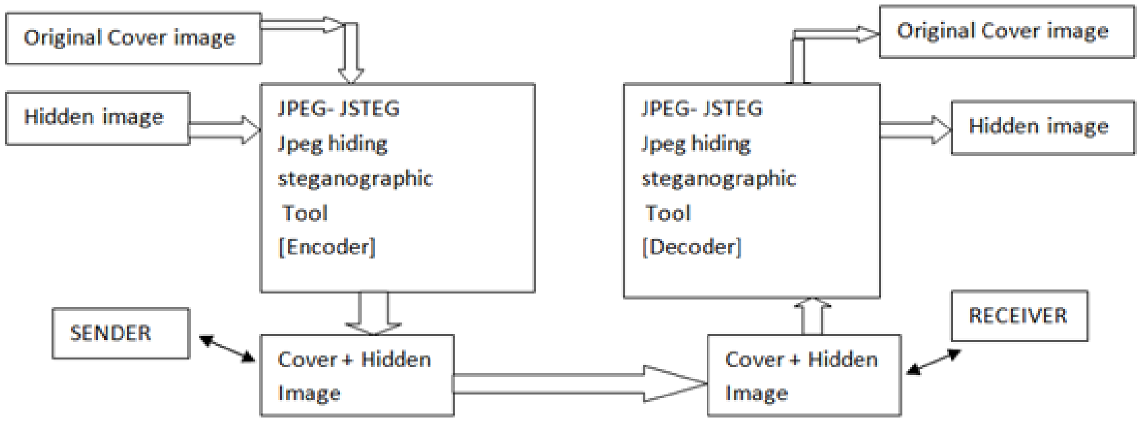


Fig.1: Diagram of image based steganography

II. Methodology

Before discussion of our proposed work we need to highlight the concept of algorithm used for data hiding i.e. Least Significant Bit insertion, working procedure of DCT and how quantization table works for JPEG images.

2.1 Improve the embedding capacity of stego image by modifying JPEG Quantization table.

To improve the quality of stego image and hiding capacity quantization table is used. It is found that quantization table provides DC coefficients that are used in image compression. So by using these tables gives more secrete data to be hidden. The default quantization table (8x8) depending upon two components named luminance and chrominance of image. But generally luminance property is change because minor change in this component is not visible in normal eyes. Default quantization table for luminance is shown in table 1.

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

Table I the default JPEG quantization table

Data hiding techniques in JPEG system, it is possible to control the image quality and compression ratio by controlling values in quantization table. Therefore, it is useful to find a quantization table with better image quality than obtained by the JPEG default tables. This implementation has to be done in our proposed work.

2.2 Spatial to Frequency domain transformation using Discrete Cosine transform (DCT).

The DCT is used in JPEG image compression and secure data hiding. There, the two-dimensional DCT of N×N blocks is computed and the results are quantized and hiding 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.

2.3 Embedding with Least Significant Bit (LSB) technique.

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, 10110110 is an 8-bit binary number. The rightmost bit '0' 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.

III. Our Proposed Work

3.1 Evaluation parameter indicates the performance of image quality

There are mainly three types of evaluation parameters through which we can be able to measure the quality of any image. In our proposed mechanism we use Modified default (8x8) quantization table in frequency domain steganography instead of Default (8x8) quantization table. In our proposed work we can evaluate the performance of image quality on the basis of following parameters.

3.1.1 Parameter-1: Square of error between cover & stego image.

This error indicates the distortion in an image.

$$\text{Mean}^2\ \text{Error}_{(Cover+Stegoimage)} = (1/\text{Size of image})^2 \sum_{i=1}^{M} \sum_{j=1}^{N} (p_c - p_s)^2$$

[Pc indicates value of pixel in cover image; Ps indicates value of pixel in stego image. Size of image = (Size of cover image (M)) X (size of stego image (N))]

3.1.2 Parameter-2: Peak Signal to noise ratio

The PSNR is most commonly used as a measure of quality of reconstruction of lossy image compression the signal in this case is the original data, and the noise is the error introduced by compression.

$$\textbf{PSNR} = 10.\log_{10} ((255^2)/\ \text{Mean}^2\ \text{Error}_{(Cover+Stegoimage)})\ \text{db}$$

3.1.3 Parameter-3: Capacity of stego image.

Maximum no of bits that can be embedded in a cover image with a negligible probability of detection by an adversary. This is called capacity which is as the size of the hidden message relative to the size of stego image. It is represented by bits per pixel and in terms of percentage.

3.2 Formation of our proposed modified default quantization table in frequency domain

Our proposed quantization table has some modification applied on default (8X8) quantization table. So by changing the values that is present in default quantization table, quality and other parameters of images are controlled. 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. [Here n is the frequency value in default 8X8 quantized table]

n/2	(n+1)/2	n/2	n/2	1	1	1	1
n/2	n/2	n/2	1	1	1	1	(n+1)/2
n/2	(n+1)/2	1	1	1	1	(n+1)/2	n/2
n/2	1	1	1	1	(n+1)/2	n/2	n/2
1	1	1	1	n/2	n/2	(n+1)/2	(n+1)/2
1	1	1	n/2	(n+1)/2	n/2	(n+1)/2	n/2
1	1	n/2	(n+1)/2	(n+1)/2	(n+1)/2	n/2	(n+1)/2
1	n/2	(n+1)/2	n/2	n/2	n/2	(n+1)/2	(n+1)/2

Table: 2. Modified proposed quantization table

3.2.1 Steps to create modified quantization table:

Step-1: The quantization table was partitioned into four bands by frequency.
Step-2: Calculate the value of a.[a=(Total no of column/2), for 8X8 table a=8/2=4]
Step-3: From 4th cell, the value of frequency is set into 1 till end in 8X8 table.
Step-4: The set of 4 consecutive 1 in row 1 is shifted left and placed in row 2.
Step-5: Step 4 is evaluated continuously for each new row till there is no place for shifting means up to 5th row.
Step-6: In 6th, 7th and 8th row are filled with frequency 1 from left to right in decreasing order.
Step-7: If the frequency value i.e. 'n' of each cell in default quantization table is even no then the value n/2 is placed on same cell in proposed modified quantization table otherwise the value (n+1)/2 is placed.

3.3 Conversion of Default (8x8) quantization table into Modified default (8x8) quantization table in frequency domain steganography.

By executing above sequential steps in section (b) we will propose a generalize table already stated in Table-2. After placing the numeric value of default table of Table -3 on that generalized table we get the modified table i.e. Table-4.

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

Table 3. Default JPEG quantization table

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

Table 4. Modified JPEG quantization table

3.4 Embedding algorithm applied to embed hidden data onto cover image at sending end.

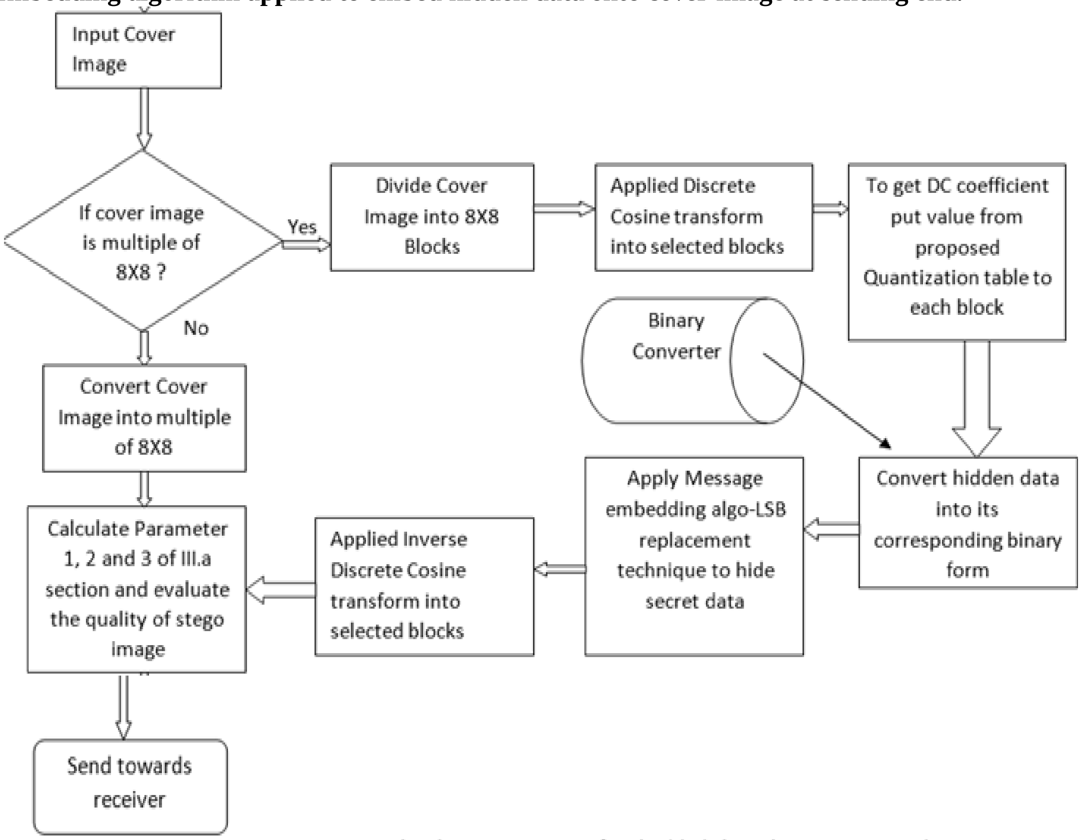
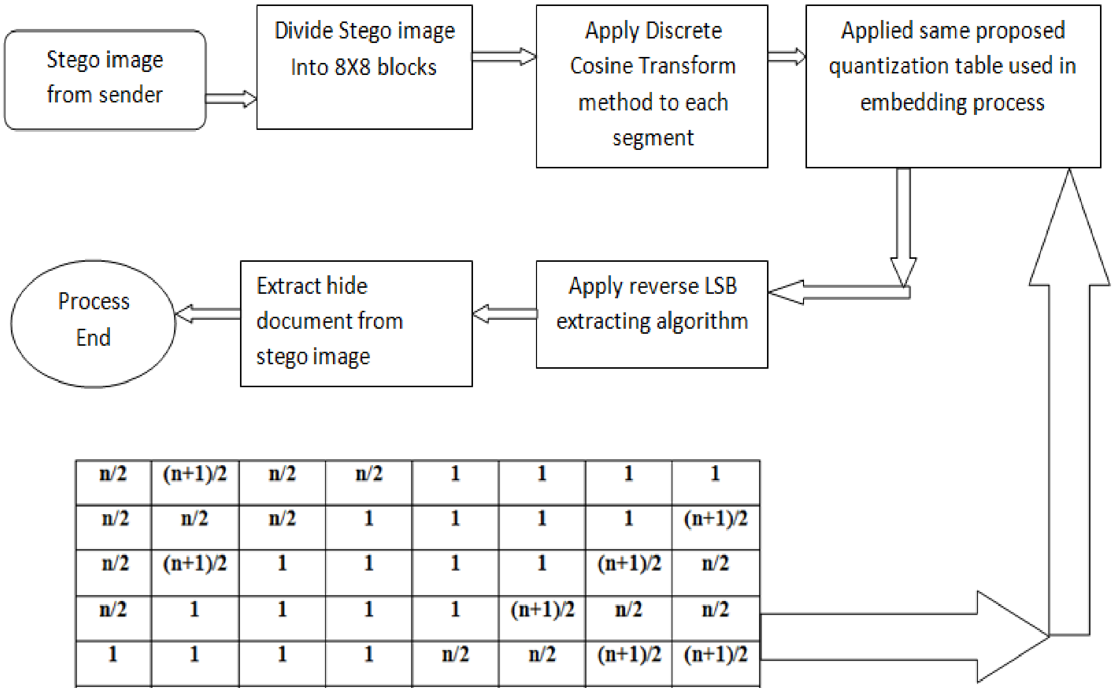


Fig. Graphical representation of embedded algorithm in SENDER side

3.5 Extracting algorithm applied to get hidden data from Stego image at receiving end.



n/2	(n+1)/2	n/2	n/2	1	1	1	1
n/2	n/2	n/2	1	1	1	1	(n+1)/2
n/2	(n+1)/2	1	1	1	1	(n+1)/2	n/2
n/2	1	1	1	1	(n+1)/2	n/2	n/2
1	1	1	1	n/2	n/2	(n+1)/2	(n+1)/2
1	1	1	n/2	(n+1)/2	n/2	(n+1)/2	n/2
1	1	n/2	(n+1)/2	(n+1)/2	(n+1)/2	n/2	(n+1)/2
1	n/2	(n+1)/2	n/2	n/2	n/2	(n+1)/2	(n+1)/2

Fig. Modified default proposed quantized table

Fig. Graphical representation of extraction algorithm in RECEIVER side

IV. Experimental Results

Results depending upon values of evaluating parameters

Image1.jpeg

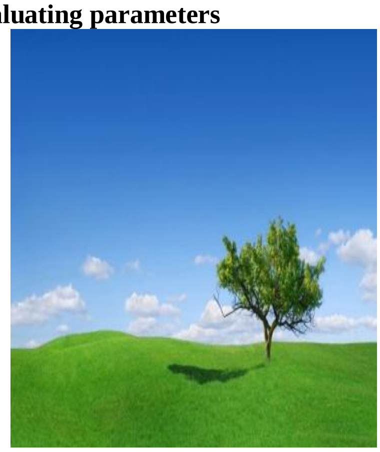
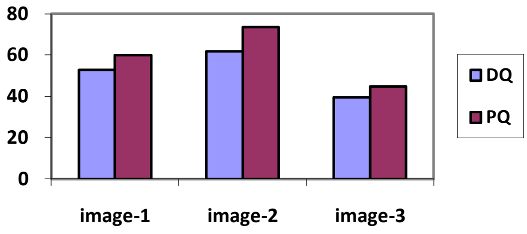


Image2.jpeg

Image.jpeg

4.1 Peak to Noise ratio calculation for both quantization tables for each sample picture.

SL.	Image name	Default Quantization	Proposed Quantization
		PSNR(db)	PSNR(db)
1.	Image1.jpeg	52.9231 db	59.833 db
2.	Image2.jpeg	61.877 db	73.395 db
3.	Image3.jpeg	39.391 db	44.7742 db

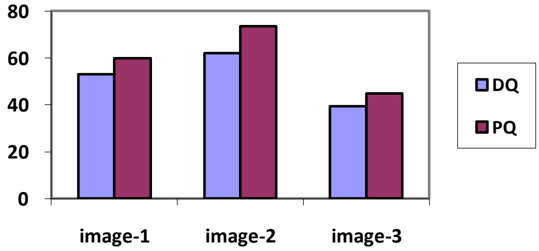


[DQ= default quantization, PQ = Proposed quantization]
Default quantization PSNR vs. modified quantization PSNR

In case of both picture the value of proposed quantization is increased than default quantization. It indicates that (PSNR of proposed quantization table > PSNR of default quantization table). So image quality has been improved.

4.2 Mean square error calculation for both quantization tables for each sample picture.

SL.	Image name	Default Quantization	Proposed Quantization
		Mean square error	Mean square error
1.	Image1.jpeg	5.2732	3.8854
2.	Image2.jpeg	3.3974	2.8219
3.	Image3.jpeg	1.1734	0.4765

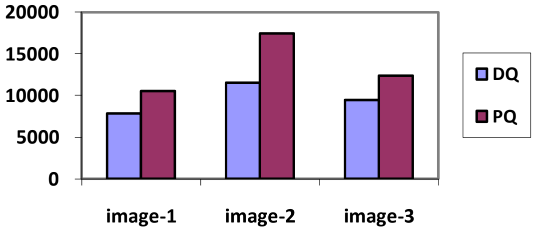


[DQ= default quantization, PQ = Proposed quantization]
Figure 2: Default quantization mean square error vs. modified quantization mean square error

In case of both picture the value of proposed quantization is decreased than default quantization. It indicates that (Mean square error of proposed quantization table < Mean square error of default quantization table). So image quality has been improved.

4.3 Capacity calculation for both quantization tables for each sample picture.

SL.	Image name	Default Quantization	Proposed Quantization
		Capacity(bits)	Capacity (bits)
1.	Image1.jpeg	7832	10569
2.	Image2.jpeg	11563	17439
3.	Image3.jpeg	9455	12347



[DQ= default quantization, PQ = Proposed quantization]
Figure 3: Default quantization capacity vs. modified quantization capacity

In case of both picture the value of proposed quantization is increased than default quantization. It indicates that (Capacity of proposed quantization table > Capacity of default quantization table). So image quality has been improved.

V. Conclusion

In this paper we are very much focused about improvement of Stego image quality by using luminance oriented modified JPEG quantization table in frequency domain approach. Similar to this image hiding limitation in LSB is overcome with LSB is associated to DCT. The stego images are obtained after hiding secret image and different parameters of stego image are calculated. In this paper we just calculate different evaluation parameters like Peak to noise ratio, Mean square error and hiding capacity of the cover image by using both quantization table (one is default 8X8 quantization table and another is our proposed modified table).According to the experimental results of our approach we can be able to increase image quality by decreasing mean square error values in frequency domain and also increasing by the capacity as well as PSNR of stego image. In our modified quantization table limits the maximum difference of Pixel value between cover and stego, so in near future also possible to maximize secret data hiding approach.

References

[1]. C.Y. Yang,―Colour Steganography based on Module Substitutions, Third International Conference on International Information Hiding & Multimedia Signal Processing Year of Publication:2007,ISBN: 0-7695-2994-1.
[2]. Li Xiaoxia, Wang Jianjun. ―A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, Vol.177, 2007, 3099-3109.
[3]. N. N. EL-Emam, ―Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm,‖ International Journal of Information and Communication Engineering, Vol.4, Issue-2, 2008.
[4]. D.C. Lou and C.H. Sung, ―A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem, IEEE TRANSACTIONS ON MULTIMEDIA, Vol. 6, No. 3, June 2004.
[5]. Li Xiaoxia, Wang Jianjun. ―A steganographic method based upon JPEG and particle swarm optimization algorithm. Information Sciences, Vol.177, 2007, 3099-3109.
[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]. 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.
[10]. W. Puech, M. Chaumont, and O. Strauss, ―A reversible data hiding method for encrypted images, Security,Forensics, Steganography, and Watermarking of Multimedia Contents X. Edited by Delp, Edward J., III; Wong, Ping Wah; Dittmann, Jana; Memon, Nasir D. Proceedings of the SPIE, Volume 6819, pp.2-5,2008.
[11]. Jiang cuiling, pang yilin, guo lun, jing bing, gong xiangyu. ―A High Capacity Steganographic Method Based on Quantization Table Modification..Wuhan University and Springer-Verlag Berlin Heidelberg, Vol.16 No.3, pp.223-227, 2011.