High Capacity Steganographic Method Based upon Quantization Error of JPEG

Dong Xiuze[1,2,3], Liu Shu[4], Zhang Ru[1,3], Niu Xinxin[1], Wang Lifeng[2]
1. Information Security Center, Beijing University of Posts and Telecommunications Beijing 100876
2. Electronic and Information Engineering Department, Beijing Electronic Science and Technology Institute Beijing 100070
3. Key Laboratory of Information Network Security，Ministry of Public Security. Shanghai 201204
4. Computer Science and Technology Department,Beijing Electronic Science and Technology Institute Beijing 100070
dongxz@besti.edu.cn

***Abstract*—Quantizing Error during the process of JPEG compression is analyzed, and a new information hiding algorithm is proposed based on Quantizing Error of JPEG image. Experimental results show that the proposed algorithm can provide a high capacity information hiding and keep the visual quality well, also the produced stego-image are almost identical to the original cover images.**

Keywords- Quantization Error, Steganography, Cover-Image, Stego-Image

I. INTRODUCTION

Steganography is the technology and art to hide the very presence of communication[1] by embedding the secret message into the innocuous-looking objects, such as digital images. JSteg[2] adopts the similar embedding scheme to the spatial LSB replacing, and is accomplished by replacing the LSB of quantized non-zero DCT coefficients. F5 [3] also embeds the message to the quantized DCT coefficients by decreasing the coefficients' absolute values。But, such steganographies, using the quantized DCT coefficients as the embedding sites, have limited capacity[4].

Tseng and Chang[5] proposed a novel steganographic method based on JPEG. The DCT for each block of 8x8 pixels was applied in order to improve the capacity and control the compression ratio. Chang et al[6]. developed a steganographic method based upon JPEG and modified 8x8 quantization table in order to improve the hiding capacity of Jpeg-Jsteg method.

Almohammad et al[7] divides the cover image into non-overlapping blocks of 16x16 pixels. For each quantized DCT block, and the least two-significant bits(2-LSBs)of each middle frequency coefficient are modified to embed two secret bits. In document [8] an information hiding method based on adjusting the JPEG quantification table is proposed, but the original image was needed to extract secret data. Furthermore, all of the above modify the quantization table of cover-image, and the modification can cause the attacker's attention. Now, we propose a novel high capacity Steganographic Method based upon quantization error of JPEG, and discuss the capacity of cover-image while not reducing the image quality.

II. QUANTIZING ERROR OF JPEG

JPEG is a commonly used method of lossy compression for digital photography (image), and the compression and decompression is as figure1. Firstly, the image should be converted from RGB into a different color space called Y′CBCR (or, informally, YCbCr). Then, the image can be divided into 8X8 block to convert to the frequency-domain representation based on discrete cosine transform (DCT), and the DCT coefficients can be quantizated using a normalized quantization table. Lastly, the quantized DC coefficient is coded by entropy coding. Contrarily, the decompression process to display the image consists of doing all the above in reverse.

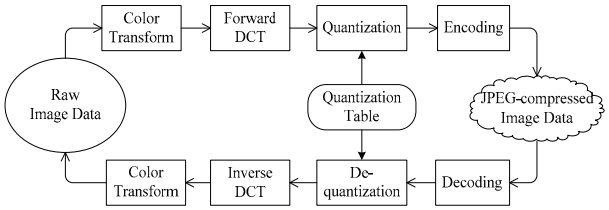

Figure 1. the process of JPEG compression and decompression based on DCT

Above the process, the process of coder and decoder is lossless, but the quantization and counter-quantization is lossy by removing redundancy. Lossy compression is necessary to achieve higher compression. In a lossy compression system, the decompressed data is not identical to the source data and much higher compression ratios can be achieved at the expense of a loss of visual quality. The difference of DCT coefficients and DCT coefficients after quantization and counter-quantization is called the Quantizing Error, which can be used to hide information.

Supposed a image divided by 8x8 block, where FI(m,n)(i,j) denotes DCT coefficients; FQ(m,n)(i,j) rounds to integer of DCT coefficients after quantization by quantization table. FD(m,n)(i,j) denotes the DCT coefficients after counter-quantization. FE(m,n)(i,j) denotes the Quantizing Error. The relationship of those symble are shown in Equ.1 to Equ.3.

$$F_Q^{(m,n)}(i,j) = sign(F_I^{(m,n)}(i,j)) \times \left\lfloor \left| F_I^{(m,n)}(i,j) \right| / Q(i,j) \right\rfloor \quad (1)$$

$$F_D^{(m,n)}(i,j) = F_Q^{(m,n)}(i,j) \times Q(i,j) \quad (2)$$

$$F_E^{(m,n)}(i,j) = F_I^{(m,n)}(i,j) - F_D^{(m,n)}(i,j) \quad (3)$$

Quantizing Error denotes information loss of JPEG compression, while Quantizing Error during certain range cannot affect the visual quality. Therefore, it can be used to hide information which has not effect on the visual quality.

III. EMBEDDING PROCEDURE

According to the above analysis result about Quantization Error, the image quality will not change significantly after we modify the original DCT coefficients FI(m,n)(i,j) to FC(m,n)(i,j), satisfied the equation Equ.4.

$$\left[F_C^{(m,n)}(i,j)/Q(i,j)\right] \equiv \left[F_I^{(m,n)}(i,j)/Q(i,j)\right] \quad (4)$$

The procedure of embedding a secret message in a cover image for Quantization Error based steganography can be described as follows:

1.The cover image is divided into non-overlapping blocks of 8×8 pixels and then the DCT is used to transform each block into DCT coefficients. The DCT block is defined as FI(m,n)(i,j).

2. Select the quality factor and quantization table and then quantized coefficients and the quantization error are calculated using Equ.1 and Equ.3.

3. Check every DCT blocks from high frequency coefficient to low ones, then, every coefficient, meeting the condition show as Equ.5, is modified by Equ.6:

$$0 < \left|F_Q^{(m,n)}(i,j)\right| \le T \le \max_{1<i,j\le 8}\left|F_Q^{(m,n)}(i,j)\right| \quad (5)$$

$$F_C^{(m,n)}(i,j) = \begin{cases} F_D^{(m,n)}(i,j) + s, F_E^{(m,n)}(i,j) \ge 0 \\ F_D^{(m,n)}(i,j) - s, F_E^{(m,n)}(i,j) < 0 \end{cases} \quad (6)$$

The feature and length of secret bit string embedded in every DCT coefficient is show in Table I.

4. Complete the Huffman encoding process, get the JPEG stego-image file.

IV. EXTRACTING PROCEDURE

Compared to embedding procedure, the procedure of extracting the embedded message form stego-images has simple steps. Only the three parameters, T, P, and Quality Factor or quantization table are needed in extracting procedure.

Embedding algorithm is described as follows.

1. After decoding the stego-image, we get the DCT coefficient $F_C^{(m,n)}(i,j)$.

2. Calculate FQ by Equ.7.

$$F_Q^{(m,n)}(i,j) = \left[F_C^{(m,n)}(i,j)/Q(i,j)\right] \quad (7)$$

3. Cruising down the coefficient matrix $F_C^{(m,n)}(i,j)$ from high frequency to the lower, for each coefficient meet the conditions that FQ < T, we can get the secret bits by Equ.8.

$$s = \left|F_C^{(m,n)}(i,j)\right| - \left|F_Q^{(m,n)}(i,j)\right| \times Q(i,j) \quad (8)$$

4. Lastly，according to the parameter P, we can get the correct length of secret bits, and then, we get the correct secret bits(may be some zero bits lie ahead).

V. EXPERIMENTAL RESULTS AND ANALYSIS

In order to evaluate the capacity and efficiency of our methods, we conducted some experiments. Six 512×512 pixels gray-level Images: Boats, airplane, Barbara, goldhill, Lenna, and Pepper were used as cover images。

Usually, Peak Signal to Noise Ratio(PSNR) and Mean Square Error (MSE) criteria are used to measure the quality of image coding and compression [9]. The PSNR for an MxN gray-level image are defined as Equ.9

$$PSNR = 10\log_{10}(M \times N \times (255)^2 \Big/ \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - X_{ij}')^2) dB \quad (9)$$

The Xi,j and Xi,j' are the pixel values of the cover image and stego-image.

The stego-images'quality and the capacity(bits)of the cover images are shown in TableII and Table III.

As Table II shows，under the same other conditions，the capacity of stego-method achieves maximum when β =1，and the capacity is the lowest when β =2. Table II also suggests that the capacity is proportional to the values of α. But in the Table III, we find that the capacity becomes smaller when the Quality Factor changed from 95% to 100%. This is because that, when Quality Factor was set to 100%, only one secret bit can be hold by every DCT coefficient.

As a gray cover image of 512×512 pixels was mentioned, the capacity of chang[5] is 52×(512×512)/(8×8) = 212,992, the capacity of Almohammad[6] is 242×(512×512)/(16×16) = 247,808, and our method can gets the max capacity to 326579.

Table III shows the comparison between the PSNR of stego_images (PSNR_S), which embedded with the max capacity, and the PSNR of the JPEG compressed (PSNR_Q) with the reference quality factor. The data indicate that，PSNR_S is always greater than PSNR_Q except use the quality factor with the value of 100，that is to say, the Quantization Error is reduced while the secret bits are embedded into the stego-images，and then the quality of stego-images are improved. As for the condition using the quality factor with the value of 100, just like described in the embedding procedures, the embedding-length is set to be 1, secret bits were embedded to the LSB of the quantized DCT coefficients.

Table IV gives the size of stego-images and compressed cover-images, the last line is the size of cover-images compressed using quality factor with the value 100, the others are stego-images' size. As we have seen, the size of stego-image are close to the compressed cover-images. That is to say, our stego-images have the similar structural characteristics with standard compressed JPEG images, won't cause the attacker's attention.

Figure 2. lenna Image (a) original image (b,c,d)stego-image when P=1,2,3

Fig.2(a) is the original images of "lenna". The least images are stego-images embedded with largest capacity by different methods. As we seen, the stego-images nice invisibility and quality.

VI. SUMMARIES

In this paper, we propose a novel steganographic method based upon Quantization Error of JPEG compression and DCT transformation, realizing the large capacity of cover-image by making full advantage of the Quantization Error. In our method, the stego-images were compressed using quality factor with the value 100, won't cause the attacker's attention. Furthermore, the original image was not needed to extract secret data. The experiment results show that, the algorithm has high capacity attribute, at the same time, the stego-image maintained a very good quality, has the very good transparency.

ACKNOWLEDGEMENT

This work is supported by 973 Project (No. 2007CB311203), the Ministry of Public Security Key Laboratory of Information Network Security, the Fundamental Research Funds for the Central Universities (BUPT2009RC02 16), the Open Funds of BESTI Key Laboratory(No. KYKF200803).

REFERENCES

[1] Lin Eugene, Delp E J. A Review of Data of Hiding in Digital Images[C]//proceedings of the Image Processing, Image Quality, Image Capture Systems Conference. Savannah, Georgia, USA:[s.n.]1999.

[2] Upham, D: Jsteg (1993) http://ftp.funet.fi/pub/crypt/cypherpunks/applications/jsteg/.

[3] WESTFELD A. "F5-A steganographic algorithm: high capacity despite better steganalysis" [C]// 4th International Workshop on Information Hiding, Lecture Notes in Computer Science. New York: Springer-Verlag, 2001, 2137:289-302.

[4] Wong PHW , Au OC , Wong JWC. "A Data Hiding Technique in JPEG Compressed Domain" [C] SPIE Conference on Security and Watermarking of Multimedia Contents III, San Jose, CA, USA, Jan 2001, vol 4314, 2001, pp. 309-340.

[5] CC. Chang, TS. Chen and L.-Z. Chung, "A steganographic method based upon JPEG and quantization table modification", Information Sciences, vol. 141, 2002, pp. 123-138

[6] Almohammad, A.; Hierons, R.M.; Ghinea, G.; "High Capacity Steganographic Method Based Upon JPEG". the Third International Conference on Availability, Reliability and Security.2008. IEEE Computer Society. pp 544-549.

[7] Bai Jianrong, Jia Yonghong, Pan Peng. "An Approach of Information Hiding Based on Adjusting JPEG Quantif ication Table", Geomatics and Information Science of Wuhan University, Vol 34 No.10, 2009, pp,1236-1239

[8] X. Kong, R. Chu, X. Ba, T. Zhang and D. Yang, "A Perception Evaluation Scheme for Steganography", in Intelligent Data Engineering and Automated Learning, vol.2690: Springer Berlin / Heidelberg, LNCS, 2003, pp. 426-430.

TABLE I. CAPACITY OF DIFFERENT STEGO-METHOD

P	**The embed message** S	**The max length of embed message** $L_{\max}$
1	consecutive Lmax secret bits	$\max(ceil(\log_2(Q(i,j)+1),1)$
2	Single bit '0', or consecutive Lmax bits starting with bit '1'	$\max(floor(\log_2 F_E^{(m,n)}(i,j)),1)$
3	Single bit '0', or consecutive Lmax bits starting with bit '1'	$\max(floor(\log_2 Q(i,j)+1),1)$

TABLE II. CAPACITY (BIT) OF QUALITY FACTOR WITH THE VALUE OF 75

	T	**P= 1**	**P= 2**	**P= 3**		**T**	**P= 1**	**P= 2**	**P= 3**
boats	4	90723	50034	67140	gold-hill	4	140999	79184	104315
	8	108135	60959	80724		8	159988	91851	119764
	12	115044	65747	86303		12	166481	96247	125353
	16	118707	67894	88996		16	169460	97942	127192
air-Plane	4	86671	48869	64246	lenna	4	94712	54346	70974
	8	102231	58414	76342		8	107377	61914	80643
	12	108807	62688	81152		12	112537	65420	84970
	16	112121	64437	84350		16	115304	67300	87310
bar-bara	4	170537	86877	122006	pepper	4	90442	52123	68391
	8	212714	111058	153052		8	102565	59652	77555
	12	222917	117101	160895		12	107498	62767	82026
	16	227948	120808	164882		16	110267	64365	83844

TABLE III. THE MAX CAPACITY AND PSNR

Quality Factor (%)	Lenna			pepper		
	Capacity (bit)	*PSNR_S (dB)*	*PSNR_Q (dB)*	*Capacity (bit)*	*PSNR_S (dB)*	*PSNR_Q (dB)*
75	120493	43.45	36.71	115970	43.70	36.29
80	137574	43.51	37.34	131529	43.89	36.79
85	155066	43.85	38.17	146547	44.41	37.49
90	174674	44.13	39.54	167412	44.36	38.85
95	251386	44.34	42.97	326579	42.44	42.82
100	256939	48.51	58.48	257095	48.54	58.45

TABLE IV. THE SIZE OF STEGO-IMAGES AND COMPRESSED COVER-IMAGES

method /image	file size(Byte)					
	boats	*airplane*	*barbara*	*goldhill*	*lenna*	*pepper*
steg_75	154,931	155,003	182,544	182,942	172,236	173,486
steg_80	155,222	155,503	182,744	183,483	172,571	173,908
steg_85	155,237	155,587	182,643	183,444	172,986	174,199
steg_90	155,663	155,694	182,338	183,620	173,118	174,502
steg_95	157,201	157,195	183,084	185,223	175,085	178,401
steg_100	165,797	166,760	189,230	191,802	181,296	182,447
JPEG_100	154,940	155,286	180,078	183,527	172,441	173.662