JPEG steganography: a performance evaluation of quantization tables

Adel Almohammad
Brunel University
adel.almohammad@brunel.ac.uk

Gheorghita Ghinea
Brunel University
george.ghinea@brunel.ac.uk

Robert M. Hierons
Brunel University
rob.hierons@brunel.ac.uk

Abstract

The two most important aspects of any image-based steganographic system are the imperceptibility and the capacity of the stego 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. Moreover, we used this optimization strategy to generate a 16x16 quantization table to be used instead of that suggested in [1]. The quality of stego-images was greatly improved when these optimized tables were used. This led us to suggest a new hybrid steganographic method in order to increase the embedding capacity. This new method is based on both [1] and Jpeg-Jsteg methods. In this method, for each 16x16 quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient are modified to embed two secret bits. Additionally, the Jpeg-Jsteg embedding technique is used for the low frequency DCT coefficients without modifying the DC coefficient. 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.

1. Introduction

Message transmissions over the Internet still have data security problems. Therefore, secure and secret communication methods are needed. Cryptography scrambles the message so that it cannot be understood. However, it makes the message suspicious enough to attract eavesdropper's attention. Steganography hides the secret message within other innocuous-looking cover files (i.e. images, music and video files) so that it cannot be observed.

There are two kinds of image steganographic techniques: spatial domain and frequency domain based methods. The schemes of the first kind directly embed the secret data within the pixels of the cover image such as Least Significant Bit (LSB) insertion.

The schemes of the second kind embed the secret data within the cover image that has been transformed such as DCT (discrete cosine transformation). The DCT coefficients of the transformed cover image are quantized, and then modified according to the secret data [10].

Capacity and stego-image quality (imperceptibility) are the two most important requirements of any steganographic system. Capacity is the amount of data embedded within a given image while the imperceptibility means that the hidden message cannot be perceived by the human visual system or other statistical means. 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 [4, 10, 11, 18, 21].

One of the most popular image formats widely used on the Internet and World Wide Web (WWW) is JPEG. JPEG compression provides a large compression ratio and maintains high image quality. Moreover, JPEG has been widely used within the steganographic community as a cover image [15, 16, 18, 19].

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 [8]. 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, 11, 12, 15, 16, 18, 19].

Although the JPEG standard uses 8x8 quantization tables, it does not specify default or standard values for quantization tables. Specifying the quantization values is left up to the application. However, the JPEG standard provides a pair of quantization tables (luminance and chrominance) as examples tested empirically and found to generate good results (Table1 for luminance). Since this quantization table is widely used, it will be called the JPEG default quantization table. However, there are

no samples for larger quantization tables in the JPEG standard.

In order to balance between image quality and compressed image size, a "Quality Scaling Factor" can be applied to the quantization table (equation (1)) [18]. Table 2 represents the default table (Table 1) but with quality factor $Q_F = 2$.

$$Q_{X,Y}' = round[\frac{Q_{X,Y}}{Q_F}] \qquad (1)$$

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 1. The default JPEG quantization table

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

Table 2. The default JPEG quantization table
$$Q_F = 2.$$

The human visual system (HVS) is more sensitive to lower frequency noise since the energy of natural images is concentrated on the lower frequency components [2]. In image compression with a JPEG baseline system, the quantization step maintains the DCT coefficients needed to achieve the desired image quality whilst it zeroes out most of high frequency DCT coefficients and discards information that is visually irrelevant [20]. Therefore, quantization table influences image quality.

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 and the compression ratio [3]. Miano states that "If you are implementing a JPEG encoder you can come up with your own scaling or use any other method you want for generating quantization values". Therefore, a quantization table can be arbitrarily generated [13]. Many different methods have been proposed to find the optimum quantization table for JPEG compression because the loss of fidelity in JPEG coding occurs entirely in the quantization step [20].

In this paper, we evaluate the impact of using optimized quantization tables (OQT) instead of the default quantization tables (DQT) on the performance of JPEG steganography. Moreover, we propose a new steganographic method with higher embedding capacity and better stego-image quality compared with the other methods tested in this paper.

The rest of this paper is organized as follows. Section 2 will review the related work on methods of JPEG steganographic and quantization tables' optimization. Section 3 will propose our data hiding scheme based upon JPEG. Section 4 will show our experimental results and will discuss the attributes of our proposed method. Finally, the conclusion will be presented in Section 5.

2. Related work

The method proposed in this paper optimizes the steganographic method of [1] in terms of capacity and stego-image quality. Moreover, it optimizes Jpeg-Jsteg and Chang et al. methods. Therefore, these methods are discussed in this section. Furthermore, the optimization methods of JPEG quantization table are described here as well.

2.1 Steganographic methods

The widely known JPEG-based steganographic tool Jpeg-Jsteg divides the cover image into non-overlapping blocks of 8x8 pixels. It embeds the secret data in the LSB of the quantized DCT coefficients of each block. Since it embeds only one bit in each quantized coefficient whose value is not 1, 0, or -1, the capacity of this method is very limited [21].

Since the energy of images is concentrated in the lower frequency coefficients, modifying such coefficients may cause a quality degradation of output image. However, high frequency coefficients will be discarded due to the quantization process. Accordingly, Chang et al. [2] developed a steganographic method based upon JPEG and modified 8x8 quantization table (Table 3) in order to improve the hiding capacity of Jpeg-Jsteg method. They utilized the middle frequency for embedding in order to achieve better hiding capacity and acceptable stego-image quality. For each quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient were modified to embed two secret bits.

In previous work [1], we proposed a steganographic method based upon JPEG compression and DCT transformation. We divided the cover image into disjoint blocks of 16x16 pixels instead of blocks of 8x8 pixels. Furthermore, we suggested a 16x16 quantization table (Table 4) and used the middle frequency coefficients for data embedding. For each quantized DCT block, the least two-significant bits (2-LSBs) of each middle frequency coefficient were modified to embed two secret bits. We got better results in terms of capacity

and imperceptibility than the previous two methods discussed.

2.2 Optimizing JPEG quantization tables

In image compression with a JPEG baseline system, it is possible to control the image quality and compression ratio by controlling values in quantization table [7]. Therefore, it is useful to find a quantization table with better image quality than obtained by the JPEG default tables [5]. We now describe some methods for optimizing the JPEG quantization table.

The relationship between quantization tables and reconstructed JPEG images' quality was investigated in [17]. 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. In another piece of work, a statistical method was used in [7] to propose a better quantization table than the default tables of JPEG compression (medical ultrasonic echo images) in order to improve the compression ratio.

In related work, Chang et al. proposed a novel

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 3. The modified quantization table of [2]

approach for designing an image independent JPEG quantization table. They derived a perceptual quantization table by incorporating the human visual system (HVS) with the uniform quantizer. This HVS-based quantization table was superior to JPEG default quantization table in terms of the perceptual quality of the reconstructed image as well as the Peak Signal-to-Noise Ratio (PSNR) [3].

Additionally, a model for generating a JPEG quantization table was proposed in [5] to improve the PSNR of the final image. The quality of the reconstructed image using this quantization table was better than the quality of image using the default JPEG quantization table.

Finally, a general strategy for modeling optimal quantization tables was presented in [14]. This method was designed for adaptive DCT image coding. Moreover, it can be used both for the JPEG image compression standard and for an extension of the JPEG approach to image block sizes other than 8x8 pixels. These optimized tables produced considerably improved compression performance compared to the default JPEG quantization table.

In conclusion, using an optimized quantization table for JPEG compression provides a reconstructed image with better quality than using the default JPEG table. Therefore, by using such optimized quantization tables, we can either get stego-images with better quality or hide more data while maintaining the stego-image quality.

3. The proposed method

The majority of research in the JPEG steganography area uses the default JPEG quantization table or a modified version of this table [2, 15, 18, 19]. However, an arbitrary and modified 16x16 quantization table was proposed in [1].

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

Table 4. The quantization table suggested by [1]

In this paper we propose a hybrid steganographic method based on both [1] and Jpeg-Jsteg. Moreover, an optimized quantization table is used instead of that arbitrary generated one. Furthermore, the impact of using such optimized quantization tables with the other stego methods is examined against the image quality and capacity.

3.1. Optimized quantization tables

Having shown the importance of the quantization table in the JPEG compression system, we are going to investigate and evaluate the effects of using optimized quantization tables on JPEG steganography.

Since we are going to optimize the steganographic method proposed in [1], we need an optimized 16x16 quantization table. The optimization strategy proposed in [14] is an appropriate method to be used because it can produce quantization tables with various dimensions rather than just 8x8 tables.

8	8	8	9	10	10	11	12
8	8	9	10	10	11	12	14
8	9	10	10	11	12	14	15
9	10	10	11	12	14	15	16
10	10	11	12	14	15	16	18
10	11	12	14	15	16	18	20
11	12	14	15	16	18	20	22
12	14	15	16	18	20	22	23

Table 5.A. The optimized quantization table

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

Table 5.B. The optimized and modified quantization table

7	7	7	7	7	7	8	8	9	9	10	11	12	13	14	15
7	7	7	7	7	8	8	9	9	10	11	12	13	14	15	17
7	7	7	7	8	8	9	9	10	11	12	13	14	15	17	18
7	7	7	8	8	9	9	10	11	12	13	14	15	17	18	20
7	7	8	8	9	9	10	11	12	13	14	15	17	18	20	22
7	8	8	9	9	10	11	12	13	14	15	17	18	20	22	24
8	8	9	9	10	11	12	13	14	15	17	18	20	22	24	26
8	9	9	10	11	12	13	14	15	17	18	20	22	24	26	28
9	9	10	11	12	13	14	15	17	18	20	22	24	26	28	30
9	10	11	12	13	14	15	17	18	20	22	24	26	28	30	33
10	11	12	13	14	15	17	18	20	22	24	26	28	30	33	36
11	12	13	14	15	17	18	20	22	24	26	28	30	33	36	39
12	13	14	15	17	18	20	22	24	26	28	30	33	36	39	42
13	14	15	17	18	20	22	24	26	28	30	33	36	39	42	45
14	15	17	18	20	22	24	26	28	30	33	36	39	42	45	49
15	17	18	20	22	24	26	28	30	33	36	39	42	45	49	52

Table 6.A. The optimized quantization table

7	7	7	7	7	1	1	1	1	1	1	1	1	1	1	1
7	7	7	7	1	1	1	1	1	1	1	1	1	1	1	17
7	7	7	1	1	1	1	1	1	1	1	1	1	1	17	18
7	7	1	1	1	1	1	1	1	1	1	1	1	17	18	20
7	1	1	1	1	1	1	1	1	1	1	1	17	18	20	22
1	1	1	1	1	1	1	1	1	1	1	17	18	20	22	24
1	1	1	1	1	1	1	1	1	1	17	18	20	22	24	26
1	1	1	1	1	1	1	1	1	17	18	20	22	24	26	28
1	1	1	1	1	1	1	1	17	18	20	22	24	26	28	30
1	1	1	1	1	1	1	17	18	20	22	24	26	28	30	33
1	1	1	1	1	1	17	18	20	22	24	26	28	30	33	36
1	1	1	1	1	17	18	20	22	24	26	28	30	33	36	39
1	1	1	1	17	18	20	22	24	26	28	30	33	36	39	42
1	1	1	17	18	20	22	24	26	28	30	33	36	39	42	45
1	1	17	18	20	22	24	26	28	30	33	36	39	42	45	49
1	17	18	20	22	24	26	28	30	33	36	39	42	45	49	52

Table 6.B. The optimized and modified quantization table

The optimized tables of Monro and Sherlock are represented by a three parameter model as following [14]:

For 8x8 blocks: $\quad Q_{xy} = A + Dz^F \quad$ (2)

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;

$$A = 5.43 + 2.15C_R$$

$$D = 0.0969 - 0.0565C_R + 0.00749C_R^2$$

$$F = 1.83$$

For 16x16 blocks: $x \rightarrow 7x/15$ and $y \rightarrow 7y/15$

$$A = 10.7 + 1.34C_R$$

$$D = -0.129 + 0.0117C_R + 0.00188C_R^2$$

$$F = 2.70$$

Equation (2) is used to generate the optimized 8x8 and 16x16 quantization tables. In order to get approximately the same compression ratio as with the default quantization table, we selected the compression ratio to be $C_R = 12$ and the quality factor to be $Q_F = 4$ (Table 5.A and Table 6.A).

3.2. The embedding and extracting procedures

The procedure of embedding a secret message in a cover image for our proposed steganographic method can be described as follows:

1. The message (M) to be embedded in the cover image is randomly generated.
2. The cover image is divided into non-overlapping blocks of 16x16 pixels and then the DCT is used to transform each block into DCT coefficients.
3. The DCT coefficients are scaled by the optimized and modified 16x16 quantization table (Table 6.B). In this quantization table, the values of (1) represent the middle frequencies to be used for embedding (242 bits). The quantized DCT coefficients of each block are rounded to the nearest integers and then set in zigzag scan order.
4. Jpeg-Jsteg embedding is applied to the low frequency coefficients (top left part, 14 coefficients, of each block) without using the DC coefficient for embedding.
5. The least two-significant bits of each middle frequency coefficient in the quantized DCT blocks are modified to embed two secret bits.
6. The JPEG entropy coding (DPCM, Run-Length coding, and Huffman coding) is applied to compress these resultant blocks, and then the JPEG file is obtained.

In our method, the procedure of extracting the embedded message from the JPEG can be described as follows:

- The JPEG file (stego-image) is entropy decoded using the coding tables (Huffman tables) located in the image header. As a result we get the blocks of quantized DCT coefficients modified according to the secret message.
- From each pre-defined middle frequency coefficient of each block we retrieve the least two-significant bits (secret bits).
- From each low frequency coefficient of each block (where its value does not equal to 0, 1, or -1), we retrieve the LSB.
- We put these retrieved bits in the same order of embedding to get the secret message (M).

4. Evaluation and discussion

Experiments were conducted in order to evaluate the efficiency of our method. Five gray-level images: Lena, Tiffany, Couple, Peppers, and Baboon (Fig 1, Fig 2, Fig 3, Fig 4, and Fig 5 respectively), each of 512x512 pixels were used as cover images.

Fig 1. Lena Image   **Fig 2. Tiffany Image**

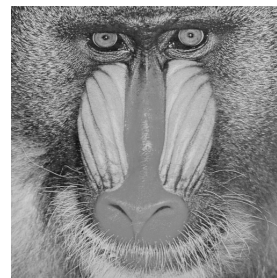**Fig 3. Couple Image**   **Fig 4. Peppers Image**

Fig 5. Baboon Image

Method (Table) / Image	Lena	Tiffany	Couple	Pepper	Baboon
Jpeg-Jsteg. (DQT)	21917	20939	31006	21042	51554
Jpeg-Jsteg (OQT)	21607	21590	33508	20395	68373
[2] (DQT)	212992	212992	212992	212992	212992
[2] (OQT)	212992	212992	212992	212992	212992
[1]	247808	247808	247808	247808	247808
[1] (OQT)	247808	247808	247808	247808	247808
Our Method (OQT)	255558	255283	257298	256066	258977

Table 7. The capacity of steganographic methods (Bits)

Method (Table) / Image	Lena	Tiffany	Couple	Pepper	Baboon
Jpeg-Jsteg. (DQT)	33.8	32.9	31.8	32.7	27.9
Jpeg-Jsteg (OQT)	34.8	34.4	33.4	33.8	30.6
[2] (DQT)	36.9	35.4	35.2	34.9	29.8
[2] (OQT)	37.9	37.4	37	36.1	35
[1]	36.9	35.2	35	34.7	29.7
[1] (OQT)	37.6	36.4	36.3	35.3	32.5
Our Method (OQT)	37.1	36	35.8	35	32.3

Table 8. The quality of stego-images, PSNR (db)

The four methods ([1, 2], Jpeg-Jsteg, and our proposed method) were coded in Matlab R2007a (V 7.4.0) and run on a PC Pentium 4 with 1GB of RAM under the Windows XP operation system.

One of the methods used to evaluate the quality of images is the human evaluation techniques. In these techniques, humans are asked to observe some images and then to evaluate or assess the visual quality of these images. However, the visual sensitivity varies from person to another and it changes over time in anyone. Therefore, different viewers will behave differently [6]. 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 [9]. The PSNR and MSE for an NxN gray-level image are defined as [2]:

$$PSNR = 10 \cdot \log_{10} \frac{255^2}{MSE} \, db \qquad (3)$$

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{N} \sum_{j=1}^{N} \left(X_{ij} - \overline{X_{ij}}\right)^2 \qquad (4)$$

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

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

4.1 Performance evaluation

In order to evaluate the performance and efficiency of the optimized quantization tables, we used them with Jpeg-Jsteg, [2], and [1] methods. Table 7 shows the capacity (bits) of the cover images using these three methods once with the default tables (Table 2, Table 3, and Table 4 respectively) and once with the optimized tables (Table 5.A, Table 5.B, and Table 6.B respectively). The Jpeg-Jsteg method does not embed a fixed number of secret bits within a given cover image. However, the capacity varies from one block to another, so this method includes code to count the number of secret bits embedded within each cover image. The method in [2] uses the 2-LSB of each predefined middle frequency coefficient (set to be 1 in Table 3 & Table 5.B) for embedding. Each block of 8x8 pixels can embed 2x26 secret bits. Therefore, a cover image of 512x512 pixels can hold 52x (512x512)/ (8x8) =212992 secret bits. However, the method in [1] can embed 242 secret bits in each block of 16x16 pixels using the same technique (Table 4 & Table 6.B). Therefore, the capacity of a cover image of 512x512 pixels is 242x (512x512)/ (16x16) = 247808 secret bits.

Table 8 shows the quality of stego-images for these three methods. It is obvious that the quality of

all stego-images produced were considerably improved when the optimized quantization tables were used instead of the default ones.

4.2 The novel method suggested

The improvement in the stego-image quality of method [1] was exploited to increase the capacity of embedding. Therefore, we suggested the hybrid stego method which involves the technique in [1] (for the middle frequencies) along with the Jpeg-Jsteg technique (for the low frequencies without the DC coefficient).

Table 7 and Table 8 respectively show the capacity and stego-image quality of this novel stego method. Our suggested method along with the optimized quantization table (Table 6.B) can embed much more information in the cover images than other methods tested. Using our method, the quality of the produced stego-images was better than that of other methods (which use the default tables). Since the capacity and imperceptibility represent the two main requirements of any steganographic technique [22], our steganographic method provides larger embedding capacity and better stego-images' quality.

5. Conclusion and future work

In this paper, we proposed a new steganographic method to improve the imperceptibility and increase the capacity of our method previously proposed in [1]. The suggested method was based on both [1] and Jpeg-Jsteg methods. It was shown that our new method can embed considerably more secret information than other stego methods tested. Furthermore, the quality of our method's stego-images was better than that of other methods which use the default quantization tables. However, determining the optimal quantization table for steganography still represents a challenge and requires further investigation.

Almost always the color space YCbCr is used to store JPEG images. The component Y (luminance) represents the intensity of the image. However, the components Cb and Cr (chrominance) specify the blueness and redness of the image respectively. Using only the Y component in such color model (YCbCR) produces a gray-level representation of the color image [13]. Therefore, gray-level images represent special cases of color images. As a result, color images can be used as cover images but we have to take all of these components (Y, Cb, and Cr) into consideration. In this case, each of the chrominance components (Cb and Cr) should have the same coding procedures that Y component has. In our future work we will consider color images and investigate the feasibility of using the chrominance components for data hiding. Moreover, we will investigate the impact of using optimized quantization tables on the size of JPEG stego-images.

6. References

[1] A. Almohammad, R. M. Hierons and G. Ghinea, "High Capacity Steganographic Method Based Upon JPEG", *The Third International Conference on Availability, Reliability and Security. ARES08*, Barcelona, Spain, 4-7 March, 2008, pp. 544-549.

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

[3] L.-W. Chang, C.-Y. Wang and S.-M. Lee, "Designing JPEG quantization tables based on human visual system*, In Proceedings of The International Conference on Image Processing. ICIP 99,* Kobe, 24-28 October, vol.2, 1999, pp. 376-380.

[4] R. Chu, X. You, X. Kong and X. Ba, "A DCT-based image steganographic method resisting statistical attacks", *In Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing. ICASSP '04*, 17-21 May. vol. 5, 2004, pp V-953-6.

[5] L. F. Costa and A. C. P. Veiga, "Identification of the best quantization table using genetic algorithms*, IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. PACRIM 2005,* 24-26 August, 2005, pp. 570-573.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, "Digital Watermarking and Steganography-Second Edition", Burlington, MA, USA, Elsevier Inc, 2008.

[7] K. Hamamoto, "Standardization of JPEG quantization table for medical ultrasonic echo images*, In Proceedings of The 6th IEEE International Conference on Electronics, Circuits and Systems. ICECS '99.* Pavos, 5-8 September, vol.2, 1999, pp. 683-686.

[8] ISO DIS 10918-1 "Digital Compression and Coding of Continuous-Tone Still Images (JPEG)", *CCITT Recommendation T.81.*

[9] 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.

[10] Y. K. Lee and L.-H. Chen, "High capacity image steganographic model", *In IEE Proceedings on Vision, Image and Signal Processing*, June, 147(3), 2000, pp. 288-294.

[11] Y.-K. Lee and L.-H. Chen, "Secure Error-Free Steganography for JPEG Images", *International Journal of Pattern Recognition and Artificial Intelligence*, vol.17, 2003, pp. 967-981.

[12] Q. Li, C. Yu and D. Chu, "A Robust Image Hiding Method Based on Sign Embedding and Fuzzy Classification", *The Sixth World Congress on Intelligent Control and Automation, 2006. WCICA 2006*, June 21-23. 2006, pp.10050-10053.

[13] J. Miano, "Compressed Image File Formats: JPEG, PNG, GIF, XBM, BMP", Addison-Wesley, 1999.

[14] D. M. Monro and B. G. Sherlock, "Optimal Quantisation Strategy for DCT Image Compression", *In IEE Proceedings of Vision Image and Signal Processing*, 143(1), 1996, pp. 10-14.

[15] V. K. Munirajan, E. Cole and S. Ring, "Transform domain steganography detection using fuzzy inference

systems", *In Proceedings of the IEEE Sixth International Symposium on Multimedia Software Engineering*, 13-15 December, 2004, pp. 286-291.

[16] J. Rongrong, Y. Hongxun, L. Shaohui, W. Liang and S. Jianchao, "A New Steganalysis Method for Adaptive Spread Spectrum Steganography", *In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IIH-MSP '06*, Dec, 2006, pp. 365-368.

[17] T. Shohdohji, Y. Hoshino and N. Kutsuwada, "Optimization of quantization table based on visual characteristics in DCT image coding", *Computers & Mathematics with Applications*, 37(11-12), 1999, pp. 225-232.

[18] H.-W. Tseng and C.-C. Chang, "Steganography using JPEG-compressed images", *The Fourth International Conference on Computer and Information Technology. CIT '04*, 14-16 September, 2004, pp. 12-17.

[19] P. H. W. Wong and J. W. C. Wong, "A Data Hiding Technique in JPEG Compressed Domain", *In Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents III*, San Joes, CA, USA, January, vol.4314, 2001, pp. 309-340.

[20] Y. O. Yildiz, K. Panetta and S. Agaian, "New Quantization Matrices for JPEG Steganography*", In Proceedings of SPIE, Mobile Multimedia/Image Processing for Military and Security Applications,* Orlando, FL, USA, 11 April, vol. 6579, 65790D, 2007, pp. 1-11.

[21] Y.-H. Yu, C.-C. Chang and Y.-C. Hu, "Hiding secret data in images via predictive coding", *Pattern Recognition*, vol.38, 2005, pp. 691-705.

[22] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity", *Signal Processing Letters, IEEE*, vol.12, 2005, pp. 67-70.