Efficiency of Frequency Selection in JPEG Steganography

Fangjun Huang, School of Info. Sci. & Tech, Sun Yat-Sen University
Guangzhou, China, huangfj@mail.sysu.edu.cn

Hyoung Joong Kim, CIST, Korea University, Seoul, Republic of Korea, khj-
@korea.ac.kr

Dong Zhang, School of Info. Sci. & Tech, Sun Yat-Sen University Guangzhou,
China, zhangd@mail.sysu.edu.cn

***Abstract*—For joint photographic experts group (JPEG) steganography, which kinds of JPEG coefficients, i.e., the block discrete cosine transform (BDCT) coefficients that have been divided by the quantization steps and have been rounded, should be selected for data hiding is still an open problem. In this paper, we present a new frequency selection approach for JPEG steganography. Via using our new approach, only those coefficients belonging to some specific alternating current (AC) frequencies, in which the ratio of the number of non-zero JPEG coefficients to the number of all JPEG coefficients is bigger than a predetermined threshold value, are selected for data hiding. Experimental results demonstrate that the frequency selection may be an efficient way to improve the security performance of JPEG steganography.**

Keywords-JPEG steganography, frequency selection, security performance

I. INTRODUCTION

Among all approaches that have been adopted to enhance the security performance of JPEG steganography, matrix encoding and adaptive embedding are of great significance. Through matrix encoding, less alternation needs to be made on the cover image while embedding the same amount of information bits. The idea of importing matrix encoding into steganography is introduced by Crandall in [1] and firstly implemented into F5 by Westfeld [2]. Recently, some new matrix encoding strategies based on BCH (Bose, Chaudhuri and Hocquenghem) codes [3, 4], ZZW (Zhang, Zhang and Wang) codes [5], STC (Syndrome-Trellis Codes) codes [6] have been presented, which can be utilized to further improve the security performance of steganography.

The adaptive embedding is to embed the secret message bits into those pixels/coefficients of carrier image that may introduce minimal distortion. A lot of distortion rules such as perturbed quantization (PQ) [7], text-adaptive PQ (PQt) [8], energy-adaptive PQ (PQe) [8], new PQ (NPQ) [9], and some other developed PQ [4, 6, 10] have been presented, which can be utilized to find those pixels/coefficients that may introduce minimal distortion in the embedding process, and thus improve the security performance of the corresponding steganography.

Generally, the above mentioned two approaches (i.e., matrix encoding and adaptive embedding) can be combined to improve the security performance of the obtained steganography simultaneously. For example, Fridrich *et al*. combined PQ with wet paper codes [7], Kim *et al*. [11] combined PQ with modified matrix encoding (MME), Huang *et al*. [9] combined NPQ with MME, and other researchers [4, 6, 10] combined the developed PQ with BCH and STC codes, *etc*. The experiments demonstrated that with combing these two approaches, the security performance of the obtained steganography would be greatly improved.

In this paper, we present a new frequency selection approach for JPEG steganography based on our previous work [22]. According to our new approach, if the coefficients belonging to some specific AC frequencies, in which the ratio of the number of non-zero JPEG coefficients to the number of all JPEG coefficients is bigger than a predetermined threshold value, are selected for data hiding, the resisting detectability of the obtained JPEG steganography can be greatly improved. Experimental results demonstrate that via using our new approach, the obtained steganographic scheme may have higher security performance than those previously presented ones [11, 22] while using the same matrix embedding strategy.

The rest of this paper is organized as follows. In Section 2, the motivation, and the test embedding algorithm are introduced. Experimental results and analysis are given in Section 3, and the conclusion is drawn in Section 4.

II. PROPOSED FREQUENCY SELECTION APPROACH

A. Motivation of Frequency Selection

Fig. 1 illustrates the standard JPEG quantization table corresponding to the quality factor (QF) of 80, in which different frequencies are associated with different quantization steps. As we know, the inverse block discrete cosine transform (BDCT) is a linear transformation. Thus the modification to the JPEG coefficient associated with smaller quantization step may result in less distortion in stego image. Based on this observation, in JPEG steganography, the secret message bits should be embedded into those coefficients belonging to the relatively low AC frequencies.

$$\begin{bmatrix} 6 & 4 & 4 & 6 & 10 & 16 & 20 & 24 \\ 5 & 5 & 6 & 8 & 10 & 23 & 24 & 22 \\ 6 & 5 & 6 & 10 & 16 & 23 & 28 & 22 \\ 6 & 7 & 9 & 12 & 20 & 35 & 32 & 25 \\ 7 & 9 & 15 & 22 & 27 & 44 & 41 & 31 \\ 10 & 14 & 22 & 26 & 32 & 42 & 45 & 37 \\ 20 & 26 & 31 & 35 & 41 & 48 & 48 & 40 \\ 29 & 37 & 38 & 39 & 45 & 40 & 41 & 40 \end{bmatrix}$$

Fig. 1 Standard JPEG quantization table corresponding to QF = 80.

Let it be noted that although those JPEG coefficients belonging to the relatively low frequencies may result in less distortion while embedding the secret message bits, it does not mean that all the relatively low AC frequencies can be selected as the embedding bands. As we know, for JPEG images with popularly used QFs from 70 to 90, there are numerous zero JPEG coefficients in general. Even in some relatively low AC frequencies, the number of zero JPEG coefficients may be much larger than that of non-zero JPEG coefficients. If these frequencies are selected as the embedding bands, some intrinsic statistical properties belonging to the JPEG image may be disturbed. Thus in our approach, only some specific AC frequencies will be selected as the data hiding bands. Different from that in [22], in each of the selected frequencies, the ratio of the number of non-zero JPEG coefficients to the number of all JPEG coefficients should be bigger than a threshold *T*. All the JPEG AC coefficients, including the zero and non-zero coefficients belonging to these selected frequencies are called changeable coefficients.

B. Test Embedding Algorighm

We assume that the raw, uncompressed image is available. Thus the JPEG coefficients, and the corresponding un-rounded BDCT coefficients (i.e., the BDCT coefficients that have been divided by quantization steps and not yet rounded) of the cover image can be obtained. The secret message bits will be embedded into the changeable JPEG coefficients under the guidance of the corresponding un-rounded BDCT coefficients.

Here, we give an example to demonstrate how to conduct our algorithm with binary Hamming codes. The secret message bits to be embedded are divided into sub-blocks with a length of *k* and the JPEG coefficients are divided into sub-blocks with a length of $2^k - 1 (k \geq 1)$. Each sub-block of *k* secret message bits will be embedded into the corresponding JPEG coefficient sub-block with the length of 2^k-1 by making at most one embedding change via using $[2^k - 1, 2^k - k - 1] (k \geq 1)$ binary Hamming codes. As seen, with a larger value of *k*, the matrix encoding will be conducted more efficiently. Note that the value of *k* is determined by the length (denoted by *L*) of all secret message bits to be embedded and the number (denoted by *N*) of JPEG coefficients that can be utilized for data hiding, i.e., $\frac{L}{N} \leq \frac{k}{2^k - 1}$. As that in the schemes [2, 11, 22], we will select the value of *k* as large as possible in our algorithm. Without loss of generality, we assume that one of the secret message sub-blocks with *k* bits is represented by $M = (m_1, m_2, ..., m_k)$, and one of the changeable JPEG coefficient sub-blocks is represented by $C = (c_1, c_2, \ldots, c_{2^k - 1})$. The corresponding un-rounded BDCT coefficient block is represented by $C' = (c'_1, c'_2, \ldots, c'_{2^k - 1})$. Through conducting matrix encoding with $[2^k - 1, 2^k - k - 1]\,(k \geq 1)$ binary Hamming codes, we can find the coefficient that may need to be altered in block *C*. For any coefficient $c_q (1 \leq q \leq 2^k - 1)$ to be altered, the least significant bit (LSB) of c_q is switched in the following way:

$$s_q = \begin{cases} c_q + 1, & if \;\; c'_q \geq c_q \\ c_q - 1, & if \;\; c'_q < c_q \end{cases} \tag{1}$$

where the corresponding un-rounded BDCT coefficient c'_q is utilized as the guidance to determine how to modify the $q^{\text{-th}}$ element in C , and s_q is the $q^{\text{-th}}$ element in JPEG coefficient block after having been modified.

In the same way, all the secret message bits can be embedded into the changeable JPEG coefficients block by block. The message extraction is the reverse process of embedding, and the embedded message can be extracted easily.

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section, experimental results and analysis are presented to demonstrate the embedding efficiency and security performance of our proposed frequency selection approach. The experimental results corresponding to MSS [22] and MME [11] have also been presented for a comparison. According to the largest number of allowable changing bits (2 or 3 bits in our experiments) in each block, the MME schemes are called MME2 and MME3, respectively.

The test image set consists of 5000 uncompressed images. Among them, 2631 images were taken by members of our group in different scenario with different cameras, 1543 images were downloaded from NRCS [12], and the remaining 1096 images are from CorelDraw image dataset [13]. All the 5000 images are central-cropped into the size of 512×512. The threshold *T* = 0.4, which is determined according to our various experiments. The generated stego images are with QF = 80. All secret message bits are randomly generated, and the embedding rates are represented in terms of *bpnc* (bits per non-zero JPEG coefficients) values. Our experiments demonstrate that while the embedding rate is as high as 0.20 *bpnc*, the ratio of the number of non-zero JPEG coefficients to the number of all JPEG coefficients for any selected frequency of the image in our image dataset do not switch from bigger than *T* to smaller than *T* in general. That is, the changeable coefficients can be accurately determined according to the threshold value *T* in the receiving end and there is no need to transfer the indexes of selected JPEG frequencies between the sender and receiver. Our proposed approach is practical and easy to be conducted.

A. Embedding Efficiency

Fig. 2 illustrates the average ratios of the number of non-zero JPEG coefficients to the number of all JPEG coefficients for different frequency bands. Our experiments include all the aforementioned 5000 images. The horizontal axis represents the different frequencies according to *zig-zag* scanning order, and the vertical axis represents the average ratios. It is observed from Fig. 2 that when *T* = 0.4, for JPEG images with QF = 70, 80 and 90, averagely 15, 19, 24 AC frequency bands can be utilized for data hiding. Note that in MSS [22], the first 19 relatively low frequencies are selected as the embedding bands, thus MSS may have the same matrix encoding efficiency as our new approach in general. According our testing, when QF = 80, for each image in our dataset there are about 73728 JPEG AC coefficients can be utilized for data hiding.

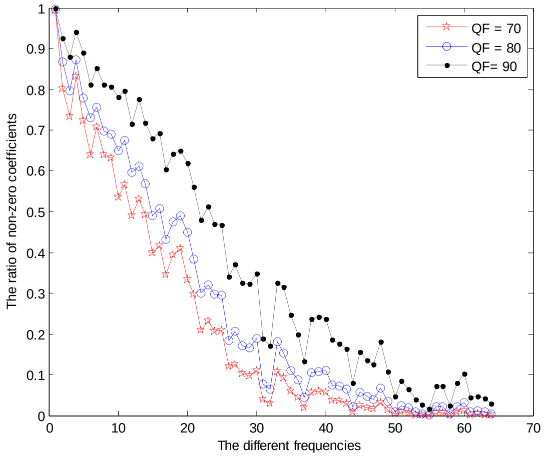

Fig. 2 The average ratios the number of non-zero JPEG coefficients to the number of all JPEG coefficients in different frequency bands

Note that in most of those previously presented JPEG steganographic schemes, e. g., F5 [2] and MME [11], only the non-zero JPEG AC coefficients are selected for data hiding. According to our testing, when QF = 80 there are about 67408 non-zero JPEG coefficients averagely. Since the numerous zero coefficients belonging to the relatively low AC frequencies are utilized for data hiding, the number of coefficients that can be utilized for data hiding in our new approach is larger than that in F5 and MME, and thus the matrix encoding efficiency can be improved, even though some non-zero JPEG coefficients belonging to the relatively high AC frequencies are excluded from data hiding.

B. Security Performance

In this sub-section, some experiments will be given to demonstrate the efficiency our proposed frequency selection approach. For comparison, we also applied MME2, MME3 and MSS with the same embedding rate to generate stego images. Note that MME2, MME3, MSS, and our proposed approach all adopt binary Hamming codes for matrix encoding. The security performance of the four JPEG steganographic schemes are tested with four universal JPEG steganalyzers presented in [14-17], denoted by ClbJFMP-274 [14], MP-486 [15], ClbMP-324 [16] and POMM-98 [17], respectively, where the numbers 274, 486, 324 and 98 denote the total number of features utilized, Clb stands for calibration technique [18], JF stands JPEG features [19], MP for Markov features [20], and POMM represents the partially ordered Markov models [17].

The support vector machine (SVM) is adopted as the classifier. For every binary classifier, the randomly selected 1/2 cover images (i.e., the JPEG compressed image without data hiding) and the corresponding 1/2 stego images are trained with the radial basis function (RBF) kernel, where the hyper-parameters (C,γ) are optimized using five-fold cross-validation over a fixed grid of values [21]. The remaining 1/2 cover and 1/2 stego images are used for testing.

The final detection accuracy rates corresponding to MME2, MME3, MSS and our approach are shown in Table 1. It is observed that our new approach has better security performance than MME2 and MME3 except in one case where the embedding rate is 0.05 *bpnc*. Note that when the embedding rate is 0.05 *bpnc*, the detection accuracy rates of MME2, MME3, and our new approach against all the aforementioned steganalyzers are nearly random guessing. When the embedding rate is no less than 0.10 *bpnc*, the security performance of our new approach are much better than that of MME2 and MME3. Table 1 shows that when the embedding rates are 0.10, 0.15 or 0.20 *bpnc*, the detection accuracy rates corresponding to our new approach will be 15-40 percent (or even further) lower than that of MME2 and MME3.

As we mentioned before, some of the frequency bands with too many zero JPEG coefficients are not suitable for data hiding. The experimental results also demonstrate that, if some of the relatively low AC frequency bands with too many zero JPEG coefficients are utilized for data hiding as in MSS [22], the security performance will be much less than our new approach, especially when ClbJFMP-274 [14] or MP-486 [15] is selected as the detector. The above experimental results demonstrate the efficiency of our new frequency selection approach.

Table 1 The detection results of F-19, F-24 and F-29 against different universal JPEG steganalyzers

bpnc	ClbJFMP-274 [14]				MP-486 [15]				ClbMP-324 [16]				POMM [17]			
	MME2	MME3	MSS	Our	MME2	MME3	MSS	Our	MME2	MME3	MSS	Our	MME2	MME3	MSS	Our
0.05	52.26	51.68	52.98	51.56	50.38	50.32	50.10	50.08	52.22	51.64	50.18	50.10	52.14	51.46	50.80	51.42
0.10	69.04	65.82	61.00	53.91	69.08	66.20	51.50	50.12	67.98	65.10	50.64	50.06	68.74	65.26	54.56	52.68
0.15	81.82	79.20	66.26	59.25	82.10	79.14	63.00	52.19	81.72	78.76	55.30	49.96	80.90	78.52	57.66	56.98
0.20	97.20	95.34	70.46	63.75	96.96	95.56	68.14	55.37	97.44	95.52	56.86	54.31	97.96	96.32	60.70	60.19

IV. CONCLUSIONS

In this paper, we have presented a new frequency selection approach. Our experimental results demonstrate that frequency selection is an important issue relating to the security performance of JPEG steganography. This new approach may have many different applications: 1) the frequency selection approach can be applied to JPEG steganography directly to improve the un-detectability of JPEG steganography for resisting today's universal JPEG steganalyzers; 2) This new idea can also be easily adopted for designing some more efficient JPEG distortion functions, e. g., since modification to those coefficients in some selected frequency may result in less distortion in the embedding process, we can associate a little cost to those coefficients while designing our new the distortion functions.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (61173147, 61100170), the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2012015587), the Fundamental Research Funds for Central Universities (12lgpy31, 12lgpy37), and the Project Sponsored by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry ([2012]1707).

REFERENCES

[1] R. Crandall, "Some notes on steganography", Posted on Steganography Mailing List, 1998. http://os.inf.tu-dresden.de/˜westfeld/crandall.pdf

[2] A. Westfeld, "High capacity despite better steganalysis (F5-a steganographic algorithm)", in Proc. Information Hiding Workshop 2001, volume 2137 of Lecture Notes in Computer Science, pp. 289-302, 2001.

[3] R. Zhang, V. Sachnev, and H. J. Kim, "Fast BCH syndrome coding for steganography," in Proc. Information Hiding Workshop 2009, volume 5806 of Lecture Notes in Computer Science, pp. 48-58, 2009.

[4] V. Sachnev, H. J. Kim, "Modified BCH data hiding scheme for JPEG steganography," Eurasip Journal on advances in signal processing, vol. 2012, no. 1, pp. 89-98, 2012

[5] W. Zhang, X. Zhang, S. Wang, "Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes, " in Proc. Information Hiding Workshop 2008, volume 5284 of Lecture Notes in Computer Science, pp. 60-71, 2008.

[6] T. Filler, J. Judas, and J. Fridrich, “Minimizing additive distortion in steganography using Syndrome-Trellis Codes,” IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 920-935, 2010.

[7] J. Fridrich, M. Goljan and D. Soukal, “Perturbed quantization steganography with wet paper codes,” in Proc. the ACM Workshop on Multimedia & Security, Magdeburg, Germany, September 20-21, pp. 4-15, 2004.

[8] J. Fridrich, T. Pevný and J. Kodovský, “Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities,” in Proc. the ACM Workshop on Multimedia and Security, Dallas, Texas, September 20-21, pp. 3-14, 2007.

[9] F. Huang, J. Huang, and Y. Q. Shi, “New channel selection rule for JPEG steganography,” IEEE Trans. Information Forensics and Security, vol. 7, no. 4, pp. 1181-1191, 2012.

[10] C. Wang, J. Ni, “An efficient JPEG steganographic scheme based on block-entropy of DCT coefficients,” in Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, Kyoto, Japan, Mar. 25-30, pp. 1785-1788, 2012.

[11] Y. Kim, Z. Duric and D. Richards, “Modified matrix encoding technique for minimal distortion steganography,” in Proc. Information Hiding Workshop 2006, volume 4437 of Lecture Notes in Computer Science, pp. 314-327, 2007.

[12] NRCS Photo Gallery. Available: http://photogallery.nrcs.usda.gov

[13] CorelDraw Image. Available: http://www.corel.com

[14] T. Pevný, J. Fridrich, “Merging Markov and DCT features for multi-class JPEG steganalysis,” in Proc. SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, pp. 650503.1-650503.13, 2007.

[15] C. Chen, Y. Q. Shi, “JPEG image steganalysis utilizing both intrablock and interblock correlations,” in Proc. IEEE International Symposium on Circuits and Systems, Seattle, WA, USA, May. 18-21, pp. 3029-3032, 2008

[16] F. Huang, J. Huang, “Calibration based JPEG steganalysis,” Science in China Series F: Information Sciences, 2009, 52(2): 260-268

[17] J. Davidson, J. Jalan, “Steganalysis using partially ordered Markov models,” in Proc. Information Hiding Workshop 2010, volume 6387 of Lecture Notes in Computer Science, pp. 118-132, 2010.

[18] J. Fridrich, M. Goljan, D. Hogea, “Steganalysis of JPEG images: Breaking the F5 algorithm,” in Proc. Information Hiding Workshop 2002, volume 2578 of Lecture Notes in Computer Science, pp. 310-323, 2002.

[19] J. Fridrich, “Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes,” in Proc. Information Hiding Workshop 2004, volume 3200 of Lecture Notes in Computer Science, pp. 67-81, 2007.

[20] Y. Q. Shi, C. Chen, W. Chen, “A Markov process based approach to effective attacking JPEG steganography,” in Proc. Information Hiding Workshop 2006, volume 4437 of Lecture Notes in Computer Science, pp. 249-264, 2007.

[21] Chang C -C, Lin C -J. LIBSVM: a library for support vector machines, 2001. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm

[22] F. Huang, Y. Q. Shi, J. Huang, “New JPEG steganographic schemes with high security performance,” in Proc. International Workshop on Digital Watermarking 2010, volume 6526 of Lecture Notes in Computer Science, pp. 189-201, 2011.

[23] J. Kodovský and J. Fridrich, “Steganalysis of JPEG images using rich models,” in Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XIV, San Francisco, CA, Jan. 23–25, 2012, vol. 8303, pp. A-1-A-13.