The ISC Int'l Journal of Information Security

ISeCure

July 2010, Volume 2, Number 2 (pp. 119–128)

http://www.isecure-journal.org

Detection of Perturbed Quantization (PQ) Steganography Based on Empirical Matrix

Mojtaba Abolghasemi [a,*], Hassan Aghaeinia [a], and Karim Faez [a]

[a] *Electrical Engineering Department, Amirkabir University of Technology, Hafez Ave., Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: 16 August 2009
Revised: 14 February 2010
Accepted: 6 April 2010
Published Online: 13 July 2010

Keywords:
Empirical Matrix, Perturbed Quantization (PQ), Steganalysis, Steganography

ABSTRACT

Perturbed Quantization (PQ) steganography scheme is almost undetectable with the current steganalysis methods. We present a new steganalysis method for detection of this data hiding algorithm. We show that the PQ method distorts the dependencies of DCT coefficient values; especially changes much lower than significant bitplanes. For steganalysis of PQ, we propose features extraction from the empirical matrix. The proposed features can be exploited within an empirical matrix of DCT coefficients which some most significant bit planes were deleted. We obtain four empirical matrices and fuse resulted features from these matrices which have been employed for steganalysis. This technique can detect PQ embedding on stego images with 77 percent detection accuracy on mixed embedding rates between $0.05 - 0.4$ bits per non-zero DCT AC coefficients (BPNZC). Comparing the results, we also show that the detection rates are effectively comparable with respect to current steganalysis techniques for PQ steganography.

1 Introduction

Information hiding has become the focus of many researches in recent years. This is the art of hiding a message signal in a host signal, such as audio, video, and still images without any imperceptible distortion of the host signal. To embed a message, the host signal is slightly modified by embedding techniques. With the broad dissemination of large amounts of digital media, the digital images have become a popular cover medium for steganography tools, and these tools can be downloaded freely from the Internet [1, 2]. In recent years, several steganographic techniques, such as Outguess [3], Model-Based (MB) [4], F5 [5], and PQ [6] have been presented for JPEG images.

Steganalysis is the art of detecting and discovering such covert messages. A steganalysis method attempts to detect the presence/absence of an embedded message, when presented with a stego signal. The huge diversity of natural images and the wide variation of data embedding algorithms make steganalysis a tough mission [7]. Several steganalysis techniques have also been proposed in the literatures. Farid *et al.* presented a general steganalysis scheme based on the high order statistics of the image in the wavelet domain [8]. They decomposed images with separable quadrature mirror filters and obtained these statistics as features for steganalysis. To attack advanced JPEG steganographic techniques, these features couldn't adequately perform steganalysis.

Shi *et al.* proposed a universal steganalysis system in [9]. The statistical moments of characteristic func-

* Corresponding author.
Email addresses: mo_abolghasemi@aut.ac.ir (M. Abolghasemi), aghaeini@aut.ac.ir (H. Aghaeinia), kfaez@aut.ac.ir (K. Faez).

ISSN: 2008-2045

tions of the image, its prediction-error image, and their discrete wavelet transform (DWT) subbands were selected as features. All of the low-low wavelet subbands were also used in their system. In [10], Fridrich developed a feature-based steganalysis (FBS) scheme. She obtained a set of distinguishing features from the DCT and spatial domains. She decompressed the JPEG image and then cropped its spatial representation by four lines of pixels in both horizontal and vertical directions and again compressed it, and estimated the statistics of the original image. She used a set of functions that operate on both spatial and DCT domains and obtained the difference between the statistics from the image and its original estimated version. The current stegnalysis methods are successful in breaking some steganography techniques such as Outguess, MB and F5, but Perturbed Quantization (PQ) steganography is a quite successful data hiding method for which current steganalysis methods failed to work [11]. In other words, the current steganalysis methods can follow. Gökhan *et al.* proposed singular value decomposition (SVD)-based features for the steganalysis of JPEG-based PQ data hiding in images [12]. They showed that JPEG-based PQ data hiding distorts linear dependencies of rows/columns of pixel values, and proposed that the features can be exploited within a simple classifier.

Sullivan *et al.* [13] presented a steganalysis technique based on the Markov chain model which captures the inter-pixel dependencies in the image. Because the size of the calculated empirical transition matrix is very large, e.g., 65536 elements for a gray-level image for a bit depth of 8, its elements cannot be used as features directly. The authors selected several largest probabilities along the main diagonal, together with their neighbors, and randomly selected some other probabilities along the main diagonal as features, resulting in a 129-dimensional (129-D) feature vector. This technique was designated to attack Spread Spectrum (SS) data hiding.

Pevny *et al.* [14] obtained a set of distinguishing features from an image and its original estimated version was obtained through a set of functions that operated on both spatial and DCT domain. They also merged these features with Markov transition features which were proposed by Shi *et al.* [15] and used these features for steganalysis of JPEG images.

Normally, natural images tend to be continuous and smooth. The correlation between adjacent pixels or their DCT coefficients is strong. The hidden data may often be independent of the cover media. The steganography process may change the continuity, causing random variations or reducing the correlation among adjacent pixels, coefficients, bitplanes and image blocks. Discovering the difference of some statistical characteristics between the cover and stego media becomes the key issue in steganalysis. Some dependencies between DCT coefficients are affected by PQ embedding due to random modifications on discrete cosine transform (DCT) coefficients. In this paper, we extract features from Empirical Matrix (denoted by EMBS) and the changes of dependencies are analyzed by the empirical matrix [16]. By a statistical hypothesis test, we justify the effectiveness of the features and then use these features to build a classifier to classify the cover and the stego-images which were embedded using the JPEG-based PQ steganography method.

The rest of the paper is organized as follows. In Section 2 we briefly review the perturbed quantization steganography and investigate its effect on bitplanes of DCT coefficients. We describe our algorithm for extraction of the features from empirical matrix in Section 3. Then in Section 4 we present experimental results and investigate the different feature vectors and their combination for steganalysis. By comparing our algorithm with other steganalysis methods, we present the results in this section. Finally, the conclusions are drawn in Section 5.

2 PQ Steganography and its Effects on Bitplanes

The PQ embedding technique was proposed by Fridrich *et al.* [7]. The quantization is perturbed according to a random key for data embedding, therefore called "Perturbed Quantization" (PQ) steganography. This method is different from its DCT-based counterparts, because it uses JPEG compression for information reducing operation. In other words, the message is embedded while the cover image undergoes compression with a lower quality factor, where only a selected set of DCT coefficients could be quantized to an alternative bin with an error smaller than some preset value. The embedding operation requires solving a set of equations in GF(2) (Galois Fields 2) arithmetics. Finding the solution to the system requires finding the rank of a $k*n$ matrix, which is computationally intensive. Therefore, to speed up the embedding process, the image is broken into blocks of smaller size, and the system is solved independently for each block. In [11], Kharrazi *et al.* measured the detection rates for three blind methods of steganalysis used on a variety of steganography schemes. The term "cover" is somewhat ambiguous for PQ JPEG hiding. The original source, from which the stego image is generated, is a once-compressed image. However, PQ is designed to mimic twice-compressed images. Because of this ambiguity, Kharrazi *et al.* measure the detection rates of two cases, with the source

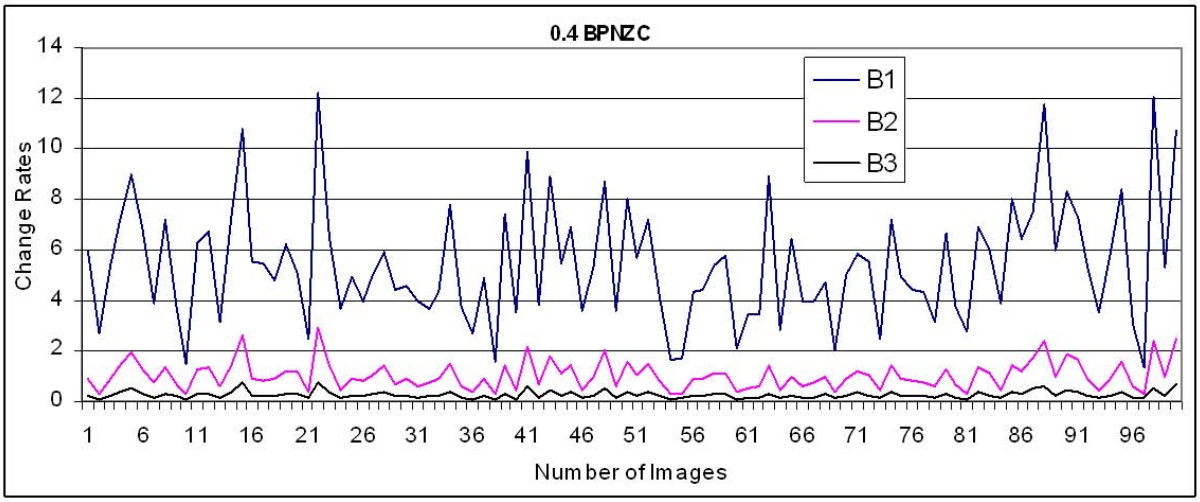


Figure 1. Changes of the first three bitplanes for 100 images due to PQ embedding (0.4 BPNZC)

(single-compressed) images and comparing with re-compressed (i.e., double-compressed) images. For the first case, the detection is found to be possible, but for the second case, it means the detection rates were essentially random. We implemented the code for this technique and obtained a stego data set created with message lengths of 0.05, 0.1, 0.2, and 0.4 BPNZC. In order to minimize the influence of the JPEG recompression, we used the recompressed images without data embedding as the cover image dataset. The re-compressed images with data embedding were used as the stego-image dataset which guarantees that the differences between the cover image and the stego-image were solely caused by the steganography itself.

In our proposed scheme, we apply a pre-processing to the image before feature extraction. This pre-processing is deletion of some of the most significant bitplanes of DCT coefficients. We investigate the embedding effects on bitplanes.

If we consider the absolute of DCT coefficients as bitplanes, most of these changes are in the lower significant bitplanes. To investigate these changes, 100 images were tested with different embedding rates. We calculate the changes of different bitplanes of these images with respect to cover images. For example the changes for the first three bitplanes (least significant bits) are shown in Figure 1 for the embedding rate of 0.4 BPNZC. Average changes for different bitplanes of DCT coefficients bitplanes are shown in Figure 2 Also the percentages of these changes are shown in table 1. As it can be noticed, most of the changes are in the least significant bitplanes of DCT coefficients, and the embedding processes have small effects on the most significant bitplanes. These changes are rapidly decreased for more than 3 bitplanes that is more than 95 percent of the changes which happened in the first 3 biteplates. Therefore we expect that the deletion of most significant bitplanes of the DCT coefficients has not affected the steganalysis performance.

Table 1. Percentage of changes on each bitplane for different embedding rates

Embedding Rate	0.1 **BPNZC**	0.2 **BPNZC**	0.4 **BPNZC**
B1	80.65	84.39	79.40
B2	14.01	11.77	15.12
B3	3.74	2.64	3.89
B4	1.07	0.76	1.07
B5	0.36	0.29	0.35
B6	0.13	0.11	0.12
B7	0.05	0.03	0.05

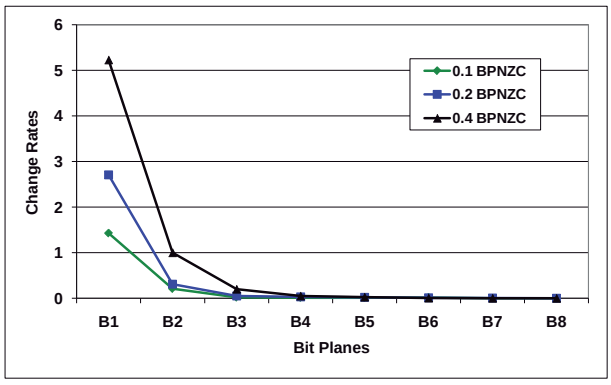


Figure 2. Average changes of each bitplanes for various embedding rates

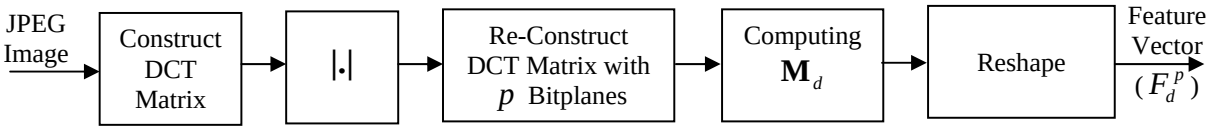


Figure 3. Feature extraction from DCT confidents

3 Proposed Steganalysis Method

In the previous work, we presented a scheme based on the empirical matrix for LSB data hiding method [17] and provided some insights that have motivated our steganalysis method in attacking PQ steganography. Specifically, we investigated higher order statistics in the DCT domain to attack PQ steganographic technique [16]. Indeed in this paper we have extended our work for steganalysis of PQ steganography.

The values of the neighbor DCT coefficients in natural images are often correlated. After the data embedding, however, the correlations between the DCT coefficients have been reduced. We consider the asymmetry of the empirical matrix and considering all elements of empirical matrix to construct the feature vector.

The empirical matrix, similar to the co-occurrence matrix can be recognized as a matrix forming the two-dimensional normalized histogram or used to estimate the joint probability mass function (PMF) of an arbitrary source. This matrix is defined over an image or its coefficients to be the distribution of co-occurring values at a given offset. Mathematically, an empirical matrix $\mathbf{M}$ is defined over an $n \times m$ matrix I, parameterized by an offset *(dx, dy)* as [18]:

$$M_d(m,n) = \{(x,y) \mid I(x,y) = m,\ I(x+dx, y+dy) = n\}$$

The proposed method is depicted in Figure 3. As it is shown, first we read the DCT coefficients from JPEG file and construct DCT matrix from 8×8 DCT blocks (Figure 4), that is, we have the DCT matrix with the same size of an image. Then we obtain the absolute DCT values and consider only p-bitplanes (p is between 1 to 4) of the DCT coefficients for reconstruction of the DCT matrix which means, for feature dimension reduction, we delete most significant bitplanes and afterward, calculate the empirical matrix. Having these bitplanes removed, in addition to obtaining feature vector with lower size, we also highlight the effects of embedding process.

As shown in Figure 4 we consider the different directions i.e., 0°, 45°, 90°, 135°, and dx=dy=d. We calculate four co-occurrence matrices, $\mathbf{M}_d^1$, $\mathbf{M}_d^2$, $\mathbf{M}_d^3$, and $\mathbf{M}_d^4$ respectively. From these matrices, we calculate the resultant co-occurrence matrix as follows:

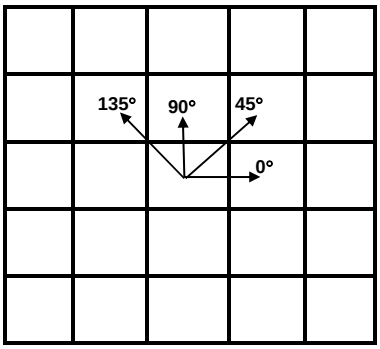


Figure 4. Construction of DCT matrix from $8*8$ DCT blocks and directions for computing empirical matrices

$$\mathbf{M}_d = (\mathbf{M}_d^1 + \mathbf{M}_d^2 + \mathbf{M}_d^3 + \mathbf{M}_d^4)/4$$

We generate the following feature vectors:

$$\begin{aligned}\mathbf{M}_d &= reshape(\mathbf{M}_d(I)) \\ &= \{D_{-2^p+1}|...|D_0|...|D_{2^p}|D_{2^p-1}\}\end{aligned}$$

Where $p = 1, 2, 3, 4$ and $d = 1, 2, 3, 4$ and *reshape* is converting the matrix to vector with concatenation of the rows of the matrix together. If we have 8 bitplanes the size of the feature vector will be 65536 and if we have 3 bitplanes the size of the feature vector will be 64.

Our algorithm for calculation of the feature vector can be summarized as following:

Algorithm Feature Calculation

Step 1. Read the DCT coefficients from JPEG file and construct a DCT matrix.

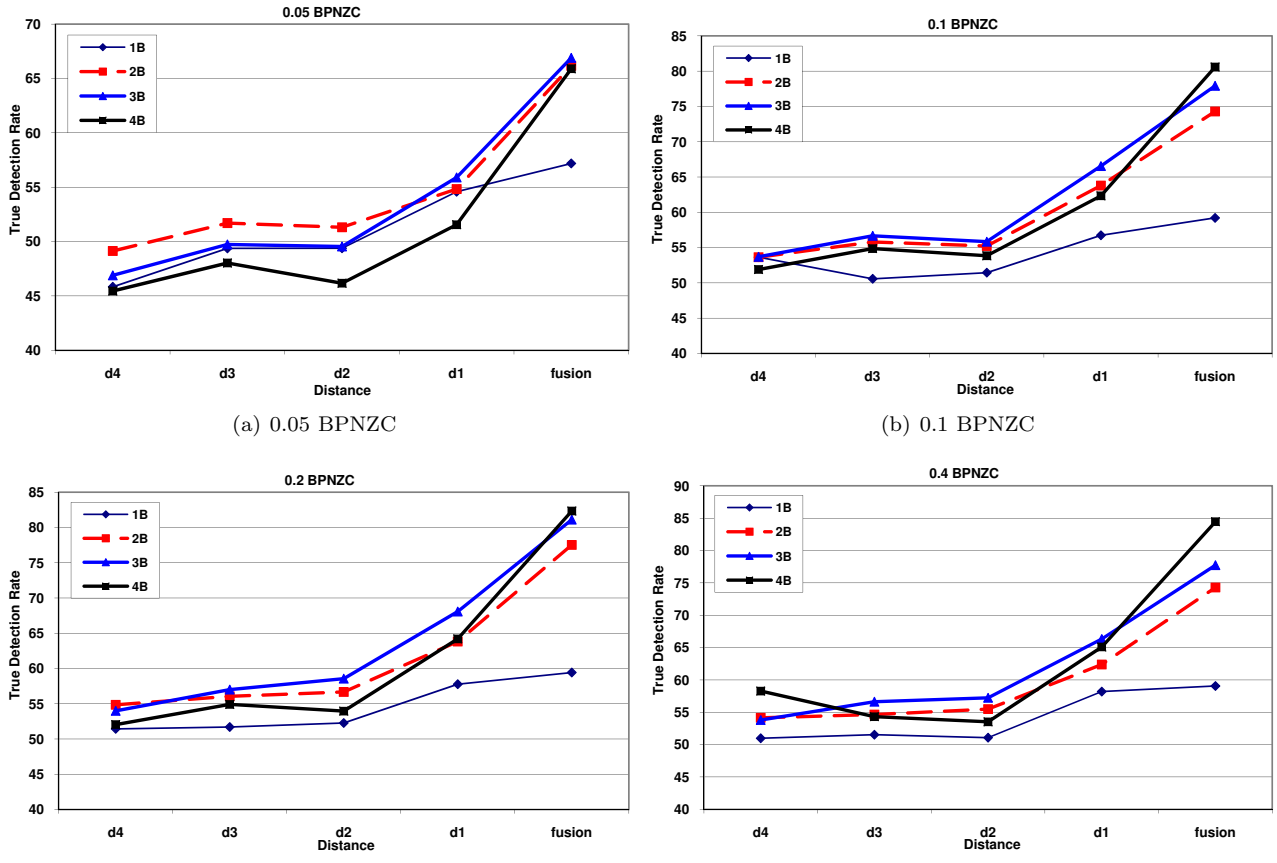
Step 2. Take the absolute values of DCT coefficients and reconstruct with least significant bit planes (Delete most significant bit planes).

Step 3. Calculate empirical matrices for different direction and obtain the mean of them and reshape each matrix to reach the feature vector.

4 Experimental Results

We used an image database partly consisting of 3000 JPEG images. Members of our research group in different places took some of these images (1650) at different time with different digital cameras. We downloaded the other 1350 images from the Internet [19].

Figure 5. Some examples of database images



(a) 0.05 BPNZC

(b) 0.1 BPNZC

(c) 0.2 BPNZC

(d) 0.4 BPNZC

Figure 6. True detection rates for different embedding rates (T=(TN+TP)/2)

The quality of images is more than 80. These images were downsized to 512×768 and were saved in BMP format. This was done to minimize JPEG compression artifacts. Then these images were converted to gray level images and were saved with factor 80 quality. These test images contained a variety of images including bright colours, reduced and dark colours, textures and fine details, and we utilized them to generate different stego images for evaluation of our method. Some of these images are shown in Figure 5. For each image in the database, we have prepared stego-images generated by the PQ JPEG steganographic technique.

Table 2. Performance for steganalysis of PQ steganography for different bitplanes and distance d (0.05 BPNZC) (TN stands for true negative rate, TP for true positive rate, and T for detection accuracy T=(TN+TP)/2)

	1B			2B			3B			4B		
	TP	NT	T	TP	NT	T	TP	NT	T	TP	NT	T
$d=1$	54.18	55.08	54.58	54.65	55.02	54.83	55.84	55.95	55.89	51.53	51.57	51.55
$d=2$	49.39	49.36	49.38	51.31	51.31	51.31	49.55	49.54	49.55	46.27	46.06	46.17
$d=3$	49.36	49.39	49.37	51.72	51.69	51.70	49.75	49.72	49.73	48.08	47.98	48.03
$d=4$	45.71	45.95	45.83	49.21	49.04	49.13	46.77	47.01	46.89	45.66	45.22	45.45
fusion	57.12	57.24	57.18	66.35	65.97	66.16	66.89	66.90	66.89	66.07	65.72	65.89

Table 3. Performance for steganalysis of PQ steganography for different bitplanes and distance d (0.1 BPNZC)

	1B			2B			3B			4B		
	TP	NT	T	TP	NT	T	TP	NT	T	TP	NT	T
$d=1$	56.22	57.36	56.74	62.43	65.48	63.79	66.23	67.53	66.86	61.70	63.04	62.33
$d=2$	51.14	51.95	51.44	54.90	55.60	55.23	55.69	55.99	55.83	55.77	53.84	53.81
$d=3$	50.37	51.18	50.57	55.62	55.98	55.80	56.15	57.28	56.67	52.51	52.90	52.69
$d=4$	53.44	53.85	53.64	53.44	53.85	53.64	52.46	53.07	52.73	48.05	48.09	48.07
fusion	59.27	59.14	59.20	73.72	74.86	74.28	78.59	77.28	77.92	80.15	81.04	80.59

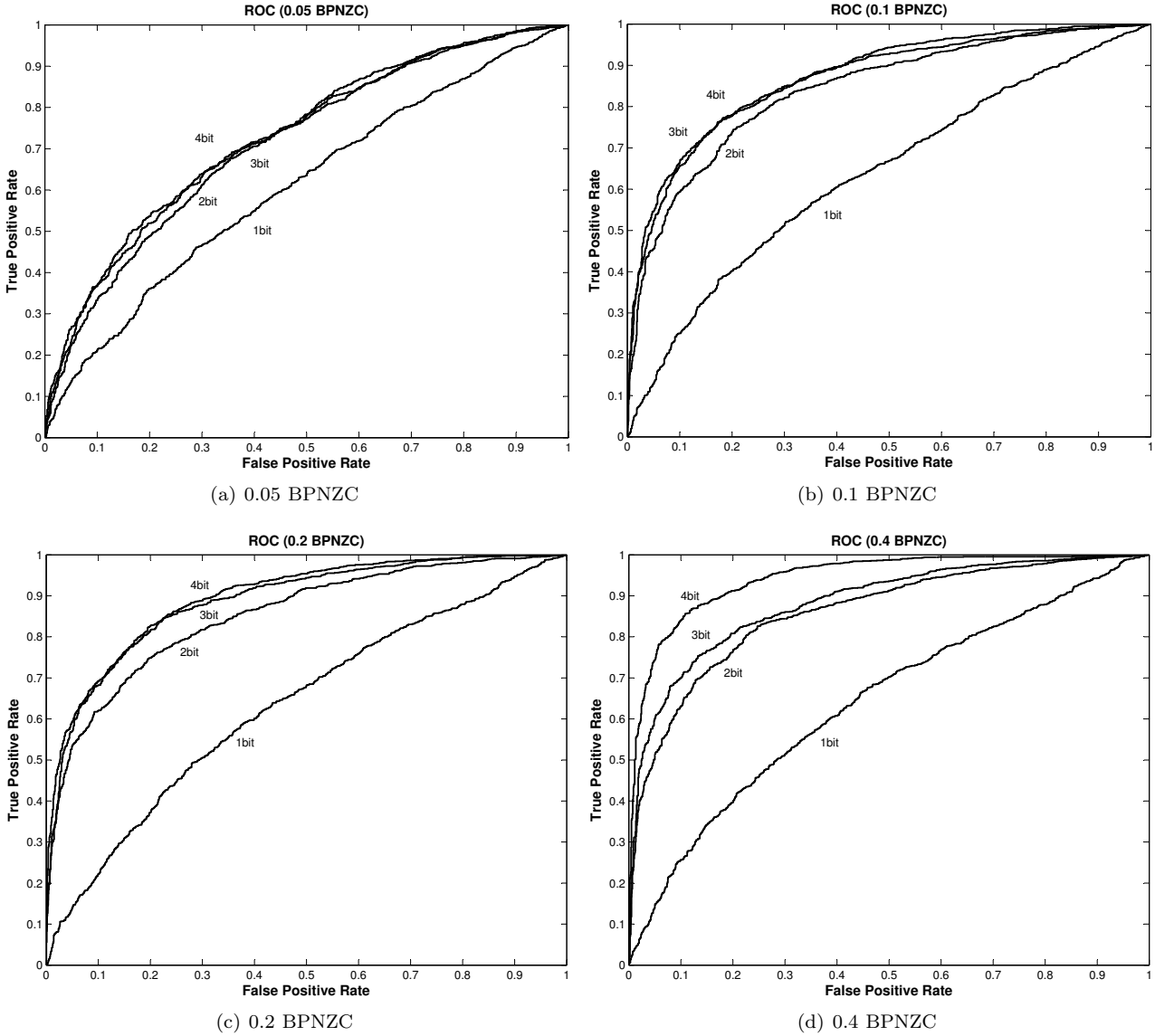
Table 4. Performance for steganalysis of steganography for different bitplanes and distance d (0.2 BPNZC)

	1B			2B			3B			4B		
	TP	NT	T	TP	NT	T	TP	NT	T	TP	NT	T
$d=1$	57.24	58.37	57.77	62.70	65.17	68.83	67.20	69.03	68.07	63.72	64.75	64.20
$d=2$	52.13	52.44	52.27	56.49	56.85	56.67	58.52	58.60	58.56	53.98	53.94	53.96
$d=3$	51.37	52.26	51.70	56.03	59.09	56.06	56.58	57.49	57.01	54.78	55.04	54.91
$d=4$	54.21	51.72	51.44	54.10	55.94	54.85	53.00	55.00	54.00	52.04	52.06	52.05
fusion	59.83	59.07	59.43	76.86	78.22	77.52	80.26	81.99	81.10	81.60	83.09	82.33

Table 5. Performance for steganalysis of PQ steganography for different bitplanes and distance d (0.4 BPNZC)

	1B			2B			3B			4B		
	TP	NT	T	TP	NT	T	TP	NT	T	TP	NT	T
$d=1$	57.24	59.45	58.20	61.29	63.74	62.39	65.81	66.88	66.33	64.34	65.95	65.09
$d=2$	51.02	51.16	51.08	55.22	55.79	55.49	57.06	57.43	57.23	53.39	53.68	53.52
$d=3$	51.25	52.10	51.53	54.40	54.94	54.64	56.23	57.10	56.63	54.23	54.41	54.32
$d=4$	50.97	51.00	50.98	53.92	54.41	54.15	53.43	54.28	58.81	57.46	59.31	58.28
fusion	59.10	59.03	59.06	74.53	74.06	74.28	77.77	77.74	77.73	86.13	82.95	84.45

As mentioned before we generated cover and stego-images with PQ for different embedding rates between 0.05 to 0.4 BPNZC.



(a) 0.05 BPNZC (b) 0.1 BPNZC

(c) 0.2 BPNZC (d) 0.4 BPNZC

Figure 7. ROC curves for different embedding rates and bitplanes

4.1 Experimental Results for Different Feature Vectors

For testing the effects of different bitplanes, we extract features for different cases. For different distances, $d = 1, 2, 3, 4$, we calculate four empirical matrices. So we have 16 feature vectors as F_d^p where $p = 1, 2, 3, 4$ and $d = 1, 2, 3, 4$. We also consider the fusion of the feature vectors by concatenating the features:

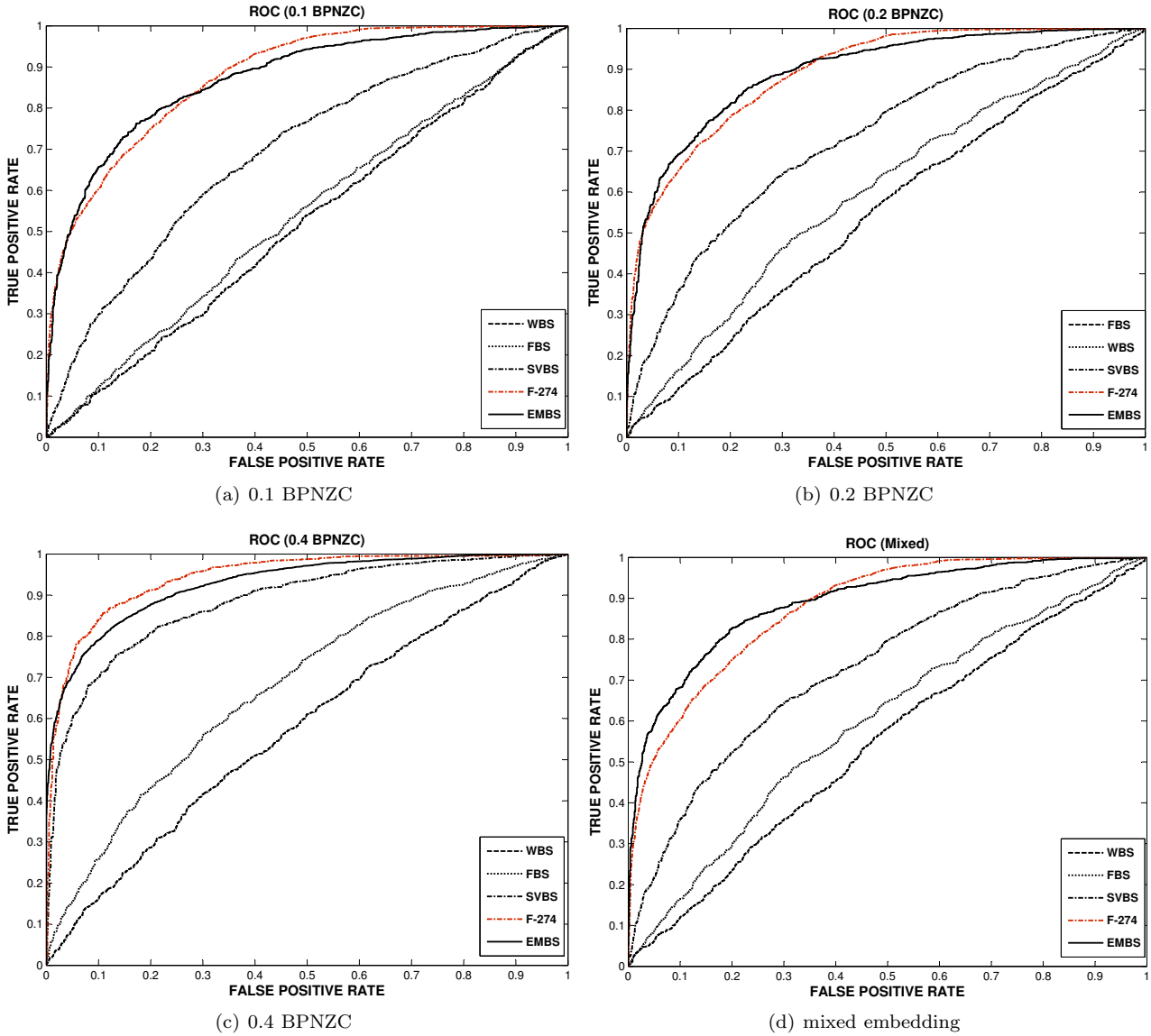
$$F_{fus} = norm\{F_1^p|F_2^p|F_3^p|F_4^p\}$$

For F_{fus} the size of the feature vector will be 4 times as large as F_d^p. We extract these features for cover and stego images with different embedding rates 0.05, 0.1, 0.2, and 0.4 BPNZC and obtain the performance results. We adopt support vector machine (SVM) with Gaussian kernel as the classifier in our experiments (MATLAB Ver. 7.3). In the classification process, we randomly select half of the original images and the corresponding half of the stego-images for training and the remaining half pairs of the cover images and stego-images for testing the trained classifier. These results are shown in Figure 6 and more detailed results are also presented in tables 2 to 5. As it can be observed, for the fusion case the performance is increased by fusing the features and considering more than one bitplanes.

Receiver operating characteristics (ROC) curves of F_{fus} are depicted in Figure 7. By considering four bitplanes, the dimension of the feature vector F_{fus} is 4×256 and we obtain 65.9, 80.6, 82.3, and 84.5 percent detection rates for 0.05, 0.1, 0.2, and 0.4 BPNZC embedding rates respectively.

Table 6. Performance for steganalysis of PQ steganography for different steganalysis methods

Embedding Rate (BPNZC)	WBS	FBS	SVBS	F-274	Proposed
0.4	61.35	64.3	78.2	85.5	84.45
0.2	53.8	54.54	76.67	81.2	82.33
0.1	50.1	51.1	71.13	79.2	80.59
0.05	49.8	50.3	68.2	63.2	65.89
Combined embedding rates	54.1	56.3	73.2	74.2	76.65



(a) 0.1 BPNZC

(b) 0.2 BPNZC

(c) 0.4 BPNZC

(d) mixed embedding

Figure 8. Comparison results. ROC curves for different embedding rates and algorithms

4.2 Comparison of the Results

In order to compare the results, we have also implemented the steganalysis schemes proposed by Shi *et al.* [9] Fridrich [10], Gökhan *et al.* [12], and Pevny *et al.* [14] (denoted by WBS, FBS, SVBS, and F-274, respectively). Then we applied them to the same set of images. The same training and testing procedures

were used and we obtained the detection rates for each case. The performance of each steganalyzer is summarized in Table 6 for different embedding rates. A ten-time repetition of the test has led to the experimental results. Also for steganalyzer techniques, the results as the receiver operating characteristics (ROC) curves are depicted in Figure 8. As it can be seen in Table 6 and Figure 8, it is clear that our proposed scheme outperforms WBS, FBS, SVBS methods by a significant margin under all embedding bit rates and comparable with F-274 algorithm for steganalysis of PQ technique.

5 Conclusions

In this paper, we have proposed an Empirical Matrix-Based Steganalysis (EMBS) method for the steganalysis of JPEG-based PQ embedding. We have shown with experimental results that the PQ embedding distorts dependencies of least significant bit planes of DCT coefficients and the empirical matrix which was computed from these bitplanes can capture these changes. The proposed features can be used for the steganalysis of JPEG-based PQ. Experimental results over images indicated the validity of the proposed scheme. The proposed steganalysis scheme outperformed the existing methods [9, 10, 12] by a significant margin under all embedding bit rates and comparable with [14] for steganalysis of PQ technique. Although the size of the features is high (4×256), other fusion techniques can be used for size reduction and performance increase. We investigated these fusion techniques for future works.

Acknowledgements

The work on this paper was supported by Iran Electronic Industrial Co. (IEI). The authors would like to thank Mehdi Kharrazi and M. A. Mehrabi for providing the source code of steganalyzers.

References

[1] Stegoarchive.com, 2009. Available at: http://stegoarchive.com.

[2] Neil F. Johnson. Steganography tools, 2009. Available at: http://www.jjtc.com/Security/stegtools.htm.

[3] N. Provos. Defending Against Statistical Steganalysis. In *Proceedings of the 10th USENIX Security Symposium*, pages 323–335, Washington DC, USA, 2001.

[4] P. Sallee. Model-based Methods for Steganography and Steganalysis. *International Journal of Image and Graphics (IJIG)*, 5(1):167–190, 2005.

[5] A. Westfeld. F5 – A Steganographic Algorithm: High Capacity Despite Better Steganalysis. In *Proceedings of the 4th Internation Workshop on Information Hiding (IH'01)*, volume 2137 of *Lecture Notes in Computer Science (LNCS)*, pages 289–302, Pittsburgh, PA, USA, 2001. Springer Verlag.

[6] J. Fridrich, M. Goljan, and D. Soukal. Perturbed Quantization Steganography with Wet Paper Codes. In *Proceedings of the ACM Workshop on Multimedia and Security*, pages 4–15, Magdeburg, Germany, 2004.

[7] R. Chandramouli, M. Kharrazi, and N. D. Memon. Image Steganography and Steganalysis: Concepts and Practice. In *Proceedings of the 2nd International Workshop on Digital Watermarking (IWDW'03)*, volume 2939 of *Lecture Notes in Computer Science (LNCS)*, pages 209–211, Seoul, Korea, 2003. Springer Verlag.

[8] H. Farid and S. Lyu. Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines. In *Proceedings of the 5th International Workshop on Information Hiding*, volume 2578 of *Lecture Noted in Computer Science (LNCS)*, pages 340–354, Noordwijkerhout, Netherlands, 2002. Springer Verlag.

[9] Y. Q. Shi, G. Xuan, D. Zou, J. Gao, C. Yang, Z. Zhang, P. Chai, W. Chen, and C. Chen. Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and Neural Network. In *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME05)*, Amsterdam, Netherlands, 2005.

[10] J. Fridrich. Feature-Based Steganalysis for JPEG Images and Its Implications. In *Proceedings of the 6th International Workshop on Information Hiding (IH'04)*, volume 3200 of *Lecture Notes in Computer Science (LNCS)*, pages 67–81, Toronto, Canada, 2005. Springer Verlag.

[11] M. Kharrazi, H. T. Sencar, and N. Memon. Performance Study of Common Image Steganography and Steganalysis Technique. *Journal of Electronic Imaging*, 15(4):041104–1–041104–16, 2006.

[12] G. Gkhan, E. D. Ahmet, and I. Avcibas. Steganalytic Features for JPEG Compression-Based Perturbed Quantization. *IEEE Signal Processing Letters*, 14(3):205–208, 2007.

[13] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath. Steganalysis for Markov Cover Data with Applications to Images. *IEEE Transactions on Information Forensics and Security*, 1 (2):275–287, 2006.

[14] T. Pevny and J. Fridrich. Merging Markov and DCT Features for Multi-Class JPEG Steganalysis.

In *Proceedings of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, pages 650503.1–650503.13, San Jose, CA, USA, 2007.

[15] Y. Q. Shi, C. Chen, and W. Chen. A Markov Process Based Approach to Effective Attacking JPEG Steganography. In *Proceedings of the 8th International Workshop on Information Hiding (IH'06)*, volume 4437 of *Lecture Notes in Computer Science (LNCS)*, pages 249–264, Alexandria, VA, USA, 2006. Springer Verlag.

[16] M. Abolghasemi, H. Aghainia, and K. Faez. Steganalysis of Perturbed Quantization (PQ) Steganography Based on Markov Chain Model. In *Proceedings of the 17th Iranian Conference on Electrical Engineering (ICEE'09)*, pages 620–625, Tehran, Iran, 2009.

[17] M. Abolghasemi, H. Aghainia, K. Faez, and M.A Mehrabi. Steganalysis of LSB Matching Based on Co-occurrence Matrix and Removing Most Significant Bit Planes. In *Proceedings of the 4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 1527–1530, Harbin, China, 2008.

[18] R. M. Haralick. Textural Features for Image Classification. *IEEE Transactions on Systems, Man and Cybernatics SMC-3*, SMC-3(6):610–621, 1973.

[19] Free Stock Photos, 2009. Available at: www.freephotos.com.

Mojtaba Abolghasemi received a B.Sc. degree in communication engineering from the University of Tabriz in Iran in 1999 and an M.Sc. degree from the Amirkabir University of Technology in 2003. He is currently a Ph.D. candidate in communication. His research interests include image processing, data hiding, and multimedia databases.

Hassan Aghaeinia received his B.Sc. degree in electronic engineering from Amirkabir University (Tehran Polytechnic) in 1987. In 1989, he finished his M.Sc. at Amirkabir University. In 1992, he received an M.Sc. from Valenciennes University (UVHC), Valenciennes, France. He then continued his studies toward a Ph.D. in electronic engineering at UVHC and completed his Ph.D. in 1996. From 1996 to the present time, he has been a faculty member at Amirkabir University, where he is an associate professor in the Communication Engineering Group. His research includes work on digital communications and spread spectrum systems, advanced communication systems, and digital image processing and image communication.

Karim Faez received his B.Sc. degree in electrical engineering, first rank, from Tehran Polytechnic University in 1973 and his M.Sc. and Ph.D. degrees in computer science from the University of California at Los Angeles (UCLA) in 1977 and 1980, respectively. Prof. Faez was with Iran Telecommunication Research Center from 1981 to 1983 before joining Amirkabir University of Technology (Tehran Polytechnic) in Iran, where he is now a professor of electrical engineering. He was the founder of the Computer Engineering Department of Amirkabir University in 1989, and he served as the first chairman from 1989 to 1992. His research interests are in pattern recognition, image processing, neural networks, signal processing, Persian (Farsi) handwriting processing, earthquake signal processing, fault tolerant system design, computer networks, and hardware design. He is a member of IEEE, IEICE, and ACM.