Science in China Series F: Information Sciences

www.scichina.com
info.scichina.com
www.springerlink.com

Calibration based universal JPEG steganalysis

HUANG FangJun[1,2†] & HUANG JiWu[1,2]

[1] School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, China;

[2] Guangdong Key Lab. of Information Security Technology, Sun Yat-Sen University, Guangzhou 510275, China

For steganalysis of JPEG images, features derived in the embedding domain appear to achieve a preferable performance. However, with the existing JPEG steganography, the minor changes due to the hidden secret data are not easy to be explored directly from the quantized block DCT (BDCT) coefficients in that the energy of the carrier image is much larger than that of the hidden signal. In this paper, we present an improved calibration-based universal JPEG steganalysis, where the microscopic and macroscopic calibrations are combined to calibrate the local and global distribution of the quantized BDCT coefficients of the test image. All features in our method are generated from the difference signal between the quantized BDCT coefficients of the test image and its corresponding microscopic calibrated image, or calculated as the difference between the signal extracted from test image and its corresponding macroscopic calibrated image. The extracted features will be more effective for our classification. Moreover, through using the Markov empirical transition matrices, both magnitude and sign dependencies along row scanning and column scanning patterns existed in intra-block and inter-block quantized BDCT coefficients are employed in our method. Experimental results demonstrate that our proposed scheme outperforms the best effective JPEG steganalyzers having been presented.

JPEG, steganography, steganalysis, microscopic calibration, macroscopic calibration

1 Introduction

Steganography is a technique which conceals the existence of hidden messages. By secretly embedding the information bits into an innocuous cover signal such as image, video, text, sound and so on, the secret message would be transmitted to the receiver without arousing suspicion. Since the JPEG image is the most common used image format today, JPEG steganography has attracted more and more attention and many JPEG steganographic algorithms have been reported[1−3].

Although the presence of the embedded messages is often imperceptible to the human eye, it may nevertheless change the statistical properties of the cover image. Because of their invasive nature, steganographic systems often leave detectable traces within some characteristics. Certainly the same is true of JPEG steganography. To attack JPEG steganography, two categories of steganalytic schemes, namely the specific steganalysis and

Received May 26, 2008; accepted November 8, 2008
doi: 10.1007/s11432-009-0033-9

†Corresponding author (email: huangfj@mail.sysu.edu.cn)

Supported by the National Basic Research Program of China (Grant No. 2006CB303104), the National Natural Science Foundation of China (Grant Nos. 90604008 and 60633030), the Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20070558054)

universal steganalysis, have been presented. Specific steganalysis concentrates on detecting some kind of particular steganographic tool[4,5], while universal steganalysis tries to steganalyze any steganographic tool[6−12]. Nowadays, many researchers pay much attention to the universal steganalysis since it can steganalyze many steganographic schemes simultaneously.

In ref. [6], Farid proposed a universal steganalyzer based on image's statistics in wavelet domain. The features are constructed from higher-order moments of the distribution of coefficients obtained using quadrature mirror filters and the prediction errors of the coefficients from several high-frequency sub-bands. Xuan et al.[7] pointed out that the defined nth statistical moment of a wavelet characteristic function is related to the nth derivative of the corresponding wavelet coefficient histogram, and hence is sensitive to data embedding. The detection results on F5 and Outguess demonstrate the effectiveness of the proposed steganalytic scheme. In ref. [8], the statistical moments of characteristic functions of the prediction-error image, the test image, and their wavelet sub-bands are chosen as the features for classification. The experimental results further demonstrate that the algorithm can provide a better performance than that in ref. [6]. These universal steganalyzers perform well in attacking steganography applied in spatial domain. However, because their features are selected from the spatial and/or wavelet transform domains, their capability in defeating JPEG steganography is rather limited.

To our knowledge, all the JPEG steganographic schemes in refs. [1–3] embed the secret message by manipulating the quantized BDCT coefficients. According to refs. [9–12], constructing the features in DCT domain may lead to a more sensitive feature set. Many new steganalytic methods in which the features are constructed mainly in the DCT domain have been presented. In ref. [9], Fridrich developed a universal steganalytic scheme specifically designed for JPEG steganography. A set of distinguishing features from the DCT domain and spatial domain are proposed. It is the first macroscopic calibrated feature set targeted for JPEG steganography, where the macroscopic calibration is an efficient process used to estimate global histogram of the quantized BDCT coefficients of the cover image from the stego image. The features are calculated as an L_1 norm of the difference between a specific macroscopic function calculated from the stego image and the same function obtained from a decompressed, cropped, and recompressed image. This scheme performs better than those in refs. [6–8] in attacking the JPEG steganographic schemes such as F5, MB1 and Outguess. In ref. [10], Shi et al. presented a new universal steganalytic scheme in which 324 features were calculated directly from the quantized BDCT coefficients. The Markov process was applied to modeling the difference JPEG coefficient matrices along horizontal, vertical and diagonal directions so as to utilize the second order statistics for steganalysis (denoted as MP-324 in this paper). The experimental results demonstrated that this scheme outperformed the methods in refs. [6, 8, 9] in attacking F5, MB1 and Outguess. Fu et al.[11] presented another universal JPEG steganalytic scheme with 200 features basically based on quantized BDCT coefficients. The Markov empirical transition matrices are used to exploit the correlations between quantized BDCT coefficients in both intra-block and row scanning inter-block sense (denoted as MP-200 in this paper). The experimental results also demonstrated its better performance in attacking F5, MB1 and Outguess compared with the methods presented in refs. [6, 8, 9]. Through extending the feature set in ref. [9] and applying calibration to the Markov features of MP-324, a new JPEG steganalyzer with 274 features is constructed in ref. [12] with markedly improved performance (denoted as JFMP-274 in this paper). However, the computation load of feature extraction in JFMP-274 is a little heavy.

In this paper, we propose a new universal JPEG steganalytic scheme. The microscopic calibration concept is presented in our method to calibrate the local distribution of the quantized BDCT coefficients. Combined with the macroscopic calibration[4,9,12] technique, a series of effective features are extracted for our classifica-

tion. Furthermore, according to ref. [13], there exist three kinds of dependencies in the quantized BDCT coefficients, i.e. intra-block correlation, inter-block correlation and sign correlation. Some recently proposed steganalyzers[10,11] only considered the correlation among the magnitude values of the BDCT coefficients since most of today's JPEG steganographic schemes do not change the sign of the quantized BDCT coefficients. However, for two coefficient pairs with the same magnitude values, e.g., (a, b) and $(a, -b)$, they may have different correlations. In our method, the Markov empirical transition matrices are used to exploit not only the magnitude but also the sign dependencies along the row scanning and column scanning patterns existed in the intra-block and inter-block quantized BDCT coefficients. Consequently, the detecting performance is further improved. The experimental results demonstrate that our proposed scheme outperforms the best effective JPEG steganalyzers having been presented.

This paper is organized as follows. In the next section, we explain how to generate the Markov empirical transition matrix first, and then describe how to achieve the microscopic and macroscopic calibrated features. The experimental results are given in section 3, and our paper is concluded in section 4.

2 Feature generation

In this section, we describe the new feature set for steganalysis of JPEG steganography. First a merged Markov empirical transition matrix on inter-block and intra-block sense is obtained, and then the matrix is calibrated using microscopic and macroscopic calibrations respectively to get our feature set for classification.

2.1 Markov empirical transition matrices generation

Without loss of generality, we suppose that the test JPEG image I_{ori} has the dimension of $M \times N$ when decompressed into spatial domain. Consider a 2-D array consisting of all of the 8×8 BDCT coefficients, which has been quantized with the quantization table and not zig-zag scanned. We call it JPEG coefficient matrix (shown in Figure 1). This JPEG coefficient matrix J_{ori} has the same size as the test image I_{ori} and thus there are $N_B = (M/8) \times (N/8)$ blocks in it. Each block has a dimension of 8×8 and all the elements are quantized BDCT coefficients. Three correlations between these quantized BDCT coefficients[13] are considered in our method by using the Markov empirical transition matrices. According to refs. [10, 11], the Markov matrices are generated as follows.

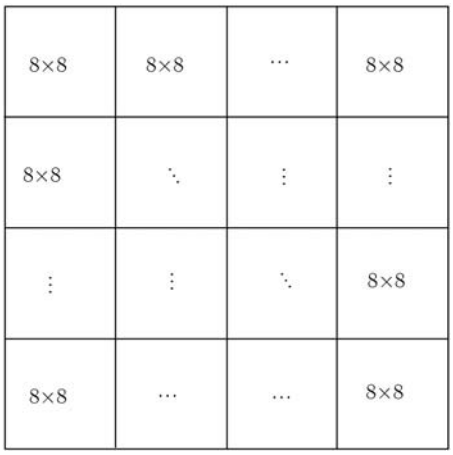

Figure 1 JPEG coefficient matrix.

1) Arrange the 8×8 blocks of the JPEG coefficient matrix J_{ori} by rows and columns respectively as shown in Figure 2. Thus two matrices with the size $8 \times (8N_B)$ can be obtained.

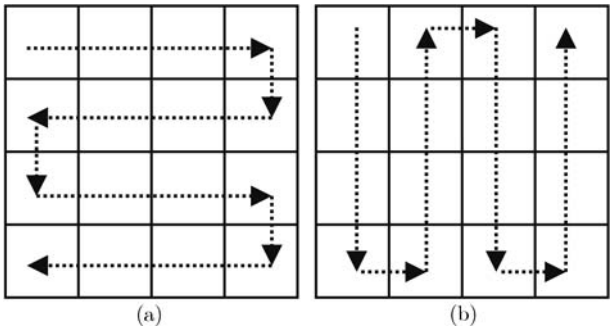

Figure 2 (a) Row scanning pattern; (b) column scanning pattern.

2) According to the zig-zag scanning pattern, expand each 8×8 quantized BDCT coefficients of the matrices got in step 1 into a 1-D column vector. The DC components are discarded and we so obtain two $63 \times N_B$ matrices J^r_{ori} and J^c_{ori}, which correspond to the row scanning pattern and column

scanning pattern respectively, as shown in Figure 2. In J^r_{ori} and J^c_{ori}, the coefficients of the same block are in the same column and the coefficients of the same frequency are in the same row.

3) Model the matrices J^r_{ori} and J^c_{ori} using Markov process. Since the elements in J^r_{ori} and J^c_{ori} have a large range, we firstly apply a thresholding technique[10,11] to reduce the feature dimension and computational complexity. In these two matrices J^r_{ori} and J^c_{ori}, if the value of an element is either larger than T or smaller than $-T$, we threshold it by T and $-T$ respectively, and the elements with the value belonging to $[-T, T]$ do not change. The Markov transition matrices are defined as follows. For any given thresholded matrix J with the size $63 \times N_B$, the dependencies between inter-block coefficients in each column are measured as[10,11]

$$\begin{aligned} &M_h(m, n; J) \\ &= p(J(i, j+1) = n | J(i, j) = m)) \\ &= \frac{\sum_{i=1}^{63} \sum_{j=1}^{N_B - 1} \delta(J(i, j) = m, J(i, j+1) = n)}{\sum_{i=1}^{63} \sum_{j=1}^{N_B - 1} \delta(J(i, j) = m)}, \end{aligned} \quad (1)$$

where $J(i, j)$ represents the coefficient value at the position (i, j) in matrix J, and $m, n \in [-T, T]$. The $\delta(x, y)$ is the impulse response function[10,11].

$$\delta(x = m, y = n) = \begin{cases} 1, & \text{if } x = m \text{ and } y = n, \\ 0, & \text{otherwise.} \end{cases}$$

Also the dependencies between intra-block coefficients in each row are measured by[10,11]

$$\begin{aligned} &M_v(m, n; J) \\ &= p(J(i+1, j) = n | J(i, j) = m) \\ &= \frac{\sum_{i=1}^{63-1} \sum_{j=1}^{N_B} \delta(J(i, j) = m, J(i+1, j) = n)}{\sum_{i=1}^{63-1} \sum_{j=1}^{N_B} \delta(J(i, j) = m)}. \end{aligned} \quad (2)$$

According to eqs. (1) and (2), the Markov empirical transition matrices $M_h(J^r_{\text{ori}})$, $M_h(J^c_{\text{ori}})$, $M_v(J^r_{\text{ori}})$ and $M_v(J^c_{\text{ori}})$ can be easily computed and there exists $M_v(J^r_{\text{ori}}) = M_v(J^c_{\text{ori}})$.

4) Since both Markov matrices $M_h(J^r_{\text{ori}})$, $M_h(J^c_{\text{ori}})$ represent the inter-block dependencies of the quantized BDCT coefficients, we adopt the average $(M_h(J^r_{\text{ori}}) + M_h(J^c_{\text{ori}}))/2$ to reduce the feature's dimension in our method.

5) Combining above Markov empirical transition matrices, we can get a new merged matrix

$$M_{\text{ori}} = [(M_h(J^r_{\text{ori}}) + M_h(J^c_{\text{ori}}))/2 \quad M_v(J^r_{\text{ori}})],$$

which has $2 \times (2T + 1) \times (2T + 1)$ elements.

2.2 Microscopic calibration

The basis of steganalysis is that there exists difference between the images before and after data hiding, and the difference is detectable. However, unknown image statistics pose a serious challenge to steganalyzers. As we know, in order to ensure that the embedded secret message is imperceptible, changes to the BDCT coefficients in JPEG steganography have been limited. According to our numerous experiments, these minor changes in the DCT domain result in a general Gaussian distributed difference between the cover and stego image in the spatial domain. Some explanation is illustrated in Figure 3, in which the histogram of the difference signal between the cover and stego images in the spatial domain is illustrated. The steganographic scheme is MB1 and embedding rate is 0.05, 0.1, 0.15, and 0.20 bpnc (bit per non-zero DCT AC coefficients), respectively.

These minor changes to the stego image are not easy to be explored since the magnitude of the quantized BDCT coefficients of the carrier image is much larger than that of the hidden signal. If we can find a gross representation of the stego image, it may be easier for us to explore the minor changes in the difference signal between the quantized BDCT coefficients of the stego image and its gross representation image. Now our main purpose is to find the same gross representation of the cover and its corresponding stego images, which is used as the microscopic calibrated image in our method. In this new microscopic calibrated image, the characteristic of the given image is preserved as much as it can be, and at the same time the minor changes due to the hidden data need be removed. Because for most of today's JPEG steganography the secret message is randomly embedded into the different frequency coefficients, the minor changes of the quantized BDCT coefficients due to the hidden data are not easy to be eliminated through a low- and/or high-pass filter in the BDCT domain. However, these minor changes can be eliminated

in spatial domain, and at the same time the gross representation of the stego image can be obtained. As mentioned in ref. [14], an important application of spatial averaging is to blur an image for the purpose of getting a gross representation of objects of interest. Since the difference signal between the cover and stego images is Gaussian distributed in spatial domain, an averaging filter can remove this effect of hidden data easily with large enough window size, at the same time almost the same gross representation of the cover and its corresponding stego image is achieved. The histogram of the difference signal between the calibrations, i.e., the gross representations of the aforementioned cover and its corresponding stego images in the spatial domain is shown in Figure 4, where the size of the

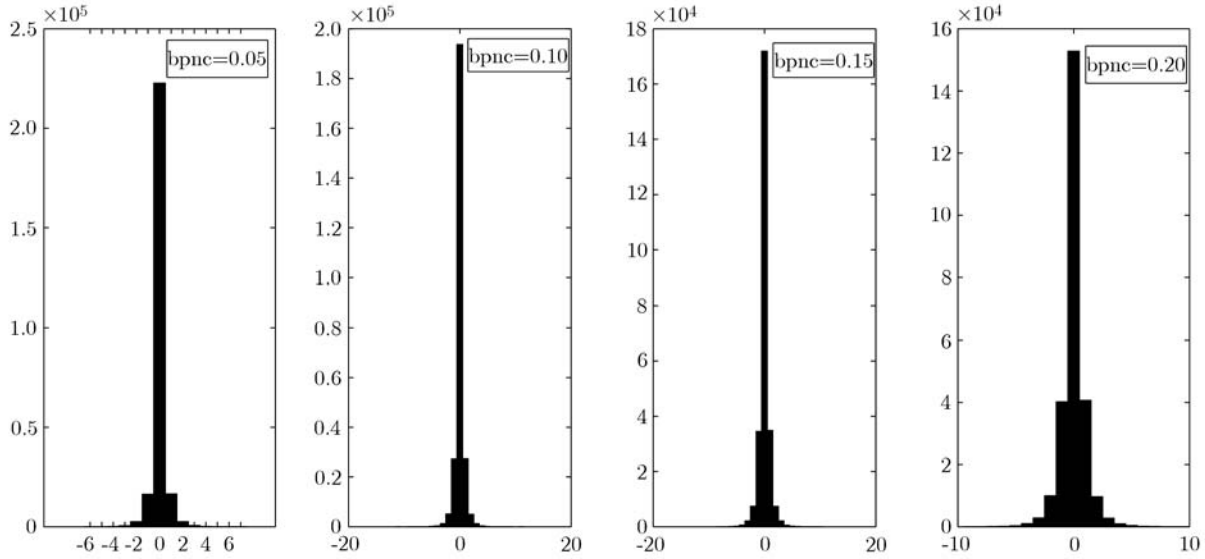

Figure 3 The histogram of the difference signal between cover and stego images for "Lena" in spatial domain.

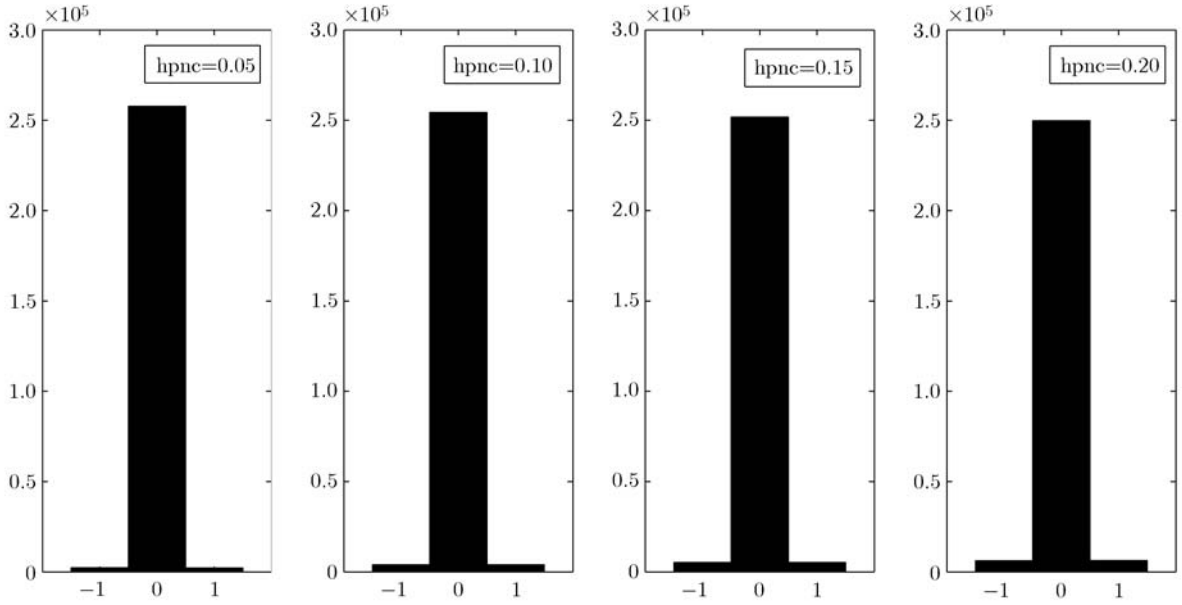

Figure 4 The histogram of the difference signal between calibrations of the cover and stego images in spatial domain.

averaging filter is 15×15. As we see, the Gaussian distributed difference, i.e., the effect of the hidden data in DCT domain, is efficiently eliminated in spatial domain, and the gross representation of the cover image has almost the same distribution as the stego's. When recompressing these calibrated versions of the cover and stego images into DCT domain again, the quantized BDCT coefficients will have almost the same distribution for each block.

The microscopic calibrated feature set is obtained as follows.

1) According to steps 1 and 2 described in section 2.1, we can get the row scanning pattern and column scanning pattern matrices J^r_{ori} and J^c_{ori} of the test JPEG image I_{ori} and its corresponding JPEG coefficient matrix J_{ori}.

2) The test JPEG image I_{ori} is decompressed into spatial domain, then manipulated by an averaging filter and recompressed again with the same quality factor as the given image. The microscopic calibrated image I_{mic} and its corresponding JPEG coefficient matrix J_{mic} can be obtained. Also according to steps 1 and 2 described in section 2.1, we can get the row scanning pattern and column scanning pattern matrices J^r_{mic} and J^c_{mic} of this new JPEG coefficient matrix J_{mic}.

3) According to steps 3 and 4 described in section 2.1, we can get the Markov empirical transition matrices $M_h(J^r_{\text{ori}} - J^r_{\text{mic}})$, $M_h(J^c_{\text{ori}} - J^c_{\text{mic}})$ and $M_v(J^r_{\text{ori}} - J^r_{\text{mic}})$.

4) The microscopic calibrated feature set is described as

$$F_{\text{mic}} = [(M_h(J^r_{\text{ori}} - J^r_{\text{mic}}) + M_v(J^c_{\text{ori}} - J^c_{\text{mic}}))/2 \quad M_v(J^r_{\text{ori}} - J^r_{\text{mic}})].$$

2.3 Macroscopic calibration

The macroscopic calibration is an efficient process used to estimate global histogram of the BDCT coefficients of the cover image from the stego image[4,9,12]. We adopt it to further improve the feature's sensitivity to the changes due to the hidden data. According to refs. [4, 9, 12], the test image I_{ori} is decompressed into spatial domain, then cropped by 4 rows and 4 columns, and recompressed again with the same JPEG quality factor as the given image. A new macroscopic calibrated spatial image I_{mac} and its corresponding JPEG coefficient matrix J_{mac} can be obtained. According to the steps described in section 2.1, we can get the merged matrix from this macroscopic calibrated image

$$M_{\text{mac}} = [(M_h(J^r_{\text{mac}}) + M_h(J^c_{\text{mac}}))/2 \ M_v(J^r_{\text{mac}})],$$

where J^r_{mac} and J^c_{mac} represent the row scanning pattern and column scanning pattern of the JPEG coefficient matrix J_{mac} respectively, and the macroscopic calibrated feature set is described as

$$\begin{aligned} F_{\text{mac}} &= M_{\text{ori}} - M_{\text{mac}} \\ &= [(M_h(J^r_{\text{ori}}) + M_h(J^c_{\text{ori}}))/2 \ M_v(J^r_{\text{ori}})] \\ &\quad - [(M_h(J^r_{\text{mac}}) + M_h(J^c_{\text{mac}}))/2 \ M_v(J^r_{\text{mac}})]. \end{aligned}$$

2.4 Merging features

The microscopic calibrated feature set F_{mic} and the macroscopic calibrated feature set F_{mac} are merged together and this new obtained feature vector $F = [F_{\text{mic}} \ F_{\text{mac}}]$ may have $4 \times (2T+1) \times (2T+1)$ elements.

3 Experimental results

In this section, we compare the performance of the proposed method with three effective universal algorithms MP-200[11], MP-324[10] and JFMP-274[12]. Our test image set consists of 4009 uncompressed images, including 1128 images taken by ourselves in different places with different cameras, 1338 images downloaded from UCID[15] and 1543 images downloaded from NRCS[16]. Since all the features in refs. [10–12] and our method are dimensionless, we test it on the images with different sizes for more reasonable results. The 1128 images taken by ourselves are with the size 512×512. The 1338 images in UCID are with the size 512×384 or 384×512 and 1543 images in NRCS are central cropped with the size 512×768 or 768×512. Some sample images are given in Figure 5. The embedded message length is represented by bpnc, i.e., bit per non-zero DCT AC coefficients. In order to avoid the influence of double JPEG and the effect introduced by different steganographic schemes, the compressed images without data embedding are used as the cover image dataset and compressed images with data embedding are used as the stego image dataset.

(a) (b) (c)

Figure 5 Sample images in our experiments. (a) Sample image taken by us; (b) sample image in UCID; (c) sample image in NRCS.

The microscopic and macroscopic calibrated images are recompressed with the same JPEG quality factor as the given image, where the JPEG quality factor can be easily achieved with JPEG Toolbox[17]. In our experiments, we choose quality factor $QF = 80$ and the threshold $T = 4$. We adopt the support vector machine (SVM) as the classifier in our works. The radial basis function (RBF) kernel is selected and the default parameters are used for the LibSVM[18]. In the classification, 7/8 randomly selected cover images and the corresponding 7/8 stego images are used as the training set, and the rest images are used for testing. The averaging filter with the size 15×15 is selected for microscopic calibration. Three publicly available steganographic schemes F5, MB1 and Outguess are tested in our experiments.

The results are shown in Table 1, where TPR, TNR represent the true positive rate and true negative rate, and AR is the final accuracy rate. The dimension of feature vector and the average feature extraction time on our computer (2.8 GHz/512 M)

Table 1 Detection rate achieved by the four steganlyzers

Algorithm	bpnc	MP-200[11]			MP-324[10]			JFMP-274[12]			Our proposed		
		TNR	TPR	AR	TNR	TPR	AR	TNR	TPR	AR	TNR	TPR	AR
F5	0.05	77.49	30.48	53.99	80.68	29.48	55.08	73.71	68.13	70.92	73.31	71.12	72.22
	0.10	77.49	61.16	69.33	76.29	58.76	67.53	91.83	90.84	91.33	92.63	91.83	92.73
	0.15	82.07	85.06	83.57	82.67	77.89	80.28	98.01	98.41	98.20	99.00	99.01	99.01
	0.20	89.64	93.03	91.34	91.04	88.45	89.75	99.60	99.60	99.60	99.80	99.60	99.70
MB1	0.05	56.18	79.88	68.03	75.10	72.31	73.71	85.06	82.47	83.77	84.26	79.48	81.87
	0.10	86.85	87.85	87.35	92.43	94.82	93.63	97.80	95.62	96.71	95.82	94.82	95.32
	0.15	95.82	95.22	95.52	98.80	99.00	98.90	99.60	98.80	99.20	98.80	99.90	99.35
	0.20	97.81	96.41	97.11	99.80	100	99.90	100	99.60	99.80	99.80	99.20	99.50
OG	0.02	69.72	38.84	54.28	67.13	53.59	60.36	83.07	83.67	83.37	86.45	85.46	85.96
	0.05	67.53	77.29	72.41	84.86	87.05	85.96	99.20	98.01	98.61	99.60	98.80	99.20
	0.08	85.46	86.06	85.76	94.22	98.21	96.22	100	99.80	99.90	100	100	100
	0.10	92.23	91.42	91.83	97.41	99.40	98.41	100	99.80	99.90	100	100	100
Features		200			324			274			324		
Time(s) per image		0.20 s			0.61 s			10.16 s			1.98 s		

for each image are given in the penultimate line and last line in Table 1 respectively. As we can see, our proposed method is much better than MP-200[11] and MP-324[10] in detecting the JPEG steganography, especially for detecting the F5 and Outguess. Also our proposed method outperforms the JFMP-274[12] in detecting the F5, Outguess and has a similar performance in detecting MB1. Moreover, though our feature dimension is larger than JFMP-274's, the feature extraction time of our method is much less than that of JFMP-274. From the last line in Table 1, we can see that for each image the average feature extraction time of our method is about 1/5 of JFMP-274's.

We also conduct the experiments with microscopic and macroscopic calibration respectively to examine the contribution made by different calibrations. The results are shown in Table 2. It is observed that the contribution made by macroscopic calibration is a little more than that of the microscopic calibration. In our future work, we will try to find some new microscopic calibration method to further improve the detection performance. Comparing Table 1 and Table 2, we can observe that combining these two calibrations has enhanced the detection rate in attacking JPEG steganography.

4 Conclusions

In this paper, we have proposed a new universal method for detection of JPEG steganography, and tested its performance on F5, MB1 and Outguess. The main contributions of this paper are as follows.

(1) We have extended the concept of calibration in steganalysis and a new method based on microscopic and macroscopic calibration is proposed to improve the detecting performance.

(2) Not only the magnitude but also the sign dependencies existed in the quantized intra-block and inter-block BDCT coefficients along row scanning and column scanning patterns are exploited by the Markov empirical transition matrices in our method.

(3) Our method can achieve the best performance compared with the steganalytic schemes reported recently.

Table 2 Detection rate with microscopic and macroscopic calibrations

Algorithm	bpnc	Microscopic calibration			Macroscopic calibration		
		TNR	TPR	AR	TNR	TPR	AR
F5	0.05	64.54	50.00	57.27	72.11	67.13	69.62
	0.10	76.29	73.90	75.10	88.45	89.05	88.75
	0.15	85.86	88.84	87.35	97.01	96.81	96.91
	0.20	93.22	97.21	95.22	99.40	99.80	99.60
MB1	0.05	73.90	75.10	74.50	81.67	78.69	80.18
	0.10	87.05	89.04	88.05	94.42	93.23	93.83
	0.15	96.22	93.03	94.63	98.61	97.81	98.21
	0.20	98.80	96.41	97.61	98.80	98.61	98.71
OG	0.02	73.71	81.87	77.79	96.61	53.78	75.20
	0.05	98.21	98.21	98.21	99.40	96.61	98.01
	0.08	99.80	100	99.90	100	99.80	99.90
	0.10	99.80	100	99.90	100	99.90	99.95

1 Westfeld A. High capacity despite better steganalysis (F5-a steganographic algorithm). In: Information Hiding, 4th International Workshop, volume 2137 of Lecture Notes in Computer Science, 2001. 289–302. Software available at http://www.rn.inf.tu-dresden.de/westfeld/f5.html
2 Sallee P. Model based methods for steganography and steganalysis. Int J Image Graphics, 2005, 5(1): 167–190. Software available at http://www.philsallee.com/mbsteg/index.html
3 Provos N. Defending against statistical steganalysis. In: 10th USENIX Security Symposium, Washington DC, USA, 2001. Software available at http://www.outguess.org
4 Fridrich J, Goljan M, Hogea, D. Steganalysis of JPEG images: Breaking the F5 algorithm. In: Information Hiding, 5th International Workshop, volume 2578 of Lecture Notes in Computer Science, 2003. 310–323
5 Böhme R, Westfeld A. Breaking Cauchy model-based JPEG steganography with first order statistics. In: 9th European Symposium on Research in Computer Security, volume 3193 of Lecture Notes in Computer Science, 2004, 125–140
6 Farid H, Siwei L. Detecting hidden messages using higher-order statistics and support vector machines. In: Information Hiding, 5th International Workshop, volume 2578 of Lecture Notes in Computer Science, 2002. 340–354
7 Xuan G, Shi Y Q, Gao J, et al. Steganalysis based on multiple features fromed by statistical moments of wavelet characteristic function. In: Information Hiding, 7th International Workshop, volume 3727 of Lecture Notes in Computer Science, 2005. 262–277
8 Shi Y Q, Xuan G, Zou D, et al. Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and nerual network. In: International Conference on Multimedia and Expro, Amsterdam, Netherlands, July 2005
9 Fridrich J. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In: Information Hiding, 6th International Workshop, volume 3200 of Lecture Notes in Computer Science, 2004. 67–81
10 Shi Y Q, Chen C, Chen W. A Markov process based approach to effective attacking JPEG steganography. In: Information Hiding, 8th International Workshop, volume 4437 of Lecture Notes in Computer Science, 2007. 249–264
11 Fu D, Shi Y Q, Zou D, et al. JPEG steganalysis using empirical transition matrix in blick DCT domain. In: International Workshop on Multimedia Signal Processing, Victoria, BC, Canada, 2006
12 Pevny T, Fridrich J. Merging Markov and DCT features for multi-class JPEG steganalysis. In: Proceedings of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, 2007, 6505: 650503-1-650503-13
13 Tu C, Tran T D. Context-based entropy coding of block transform coefficients form image compression. IEEE Trans Image Process, 2002, 11(11): 1271–1283
14 Gonzalez R C, Woods R E. Digital Image Processing. 2nd ed. Prentice Hall: Pearson Education, Inc., 2002
15 Schaefer G, Stich M. UCID——An uncompressed colour image database. Technical Report, School of Computing and Mathematics, Nottingham Trent University, UK, 2003
16 http://photogallery.nrcs.usda.gov
17 Sallee P. http://redwood.ucdavis.edu/phil/demos/jpegtbx/jpegtbx.htm
18 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