Steganalysis of adaptive JPEG steganography by selecting DCT coefficients according to embedding distortion

Xiaofeng Song, Fenlin Liu, Chunfang Yang, Xiangyang Luo and Zhenyu Li
[1] Zhengzhou Science and Technology Institute
[2] State key Laboratory of Mathematical Engineering and Advanced Computing
Zhengzhou, Henan 450001 - China
[e-mail: xiaofengsong@sina.com, chunfangyang@126.com]
*Corresponding author: Xiaofeng Song, Chunfang Yang

Received April 19, 2015; revised August 2, 2015; accepted September 28, 2015; published December 31, 2015

Abstract

According to the characteristics of adaptive JPEG steganography which determines the changed DCT coefficients based on embedding distortion, a new steganalysis method by selecting the DCT coefficients with small distortion values is proposed. Firstly, the principle of adaptive JPEG steganography through minimizing distortion is introduced. Secondly, the practicability of selecting the changed DCT coefficients according to distortion values is studied. Thirdly, the proposed steganalysis method is given and the embedding sensitivity of the steganalysis feature extracted from the selected DCT coefficients is analyzed. Lastly, the implement processes of the proposed method are presented and analyzed in details. In the experiments, PQt, PQe and J-UNIWARD steganography are used as examples to verify the effect of the proposed steganalysis method for adaptive JPEG steganography. A serial experimental results show the detection accuracy can be improved obviously, especially when the payload is relatively low.

Keywords: JPEG image, adaptive steganography, steganalysis, embedding distortion

This research was supported by a research grant from the National Natural Science Foundation of China (Grant Nos. 61272489, 61379151, 61302159, 61401512 and 61572052), the Excellent Youth Foundation of Henan Province of China (Grant No. 144100510001), the National Cryptography Development Fund of China (No.MMJJ201301005) and the Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-14-108)

http://dx.doi.org/10.3837/tiis.2015.12.026 **ISSN : 1976-7277**

1. Introduction

Image Steganography is the science and art of convert communication which try to embed the secret messages into innocuous-looking cover image [1]. The countermeasure against steganography technology is steganalysis [2] which focuses on detecting the presence of the secret messages. In recent years, with the development of Internet and steganography technologies, more and more algorithms and softwares are constantly emerging and can be got easily. It enables people to exchange their information conveniently. However, this also provides fertile grounds for illegal parties to disseminate their messages to each other secretly by utilizing steganography technologies. Therefore, image steganalysis which try to develop techniques for detecting this secret messages exchange is becoming more and more important.

JPEG is one of the most popular image formats on the internet, thus the steganography and steganalysis technology about JPEG image attract more attentions. For now, the steganography algorithms for JPEG image can be divided into non-adaptive steganography and adaptive steganography. The former includes Jsteg [3], MB1 [4], MB2 [5], Outguess [6], F5 [7], PQ (Perturbed Quantization) [8], MME (Modified Matrix Encoding) [9], nsF5 [10], etc. The latter includes PQt (texture-adaptive PQ), PQe (energy-adaptive PQ) [10], MOD (Model Optimized Distortion) [11], NPQ (Normalized Perturbed Quantization**)** [12], EBS (Entropy Block Steganography) [13], UED (Uniform Embedding Distortion) [14], J-UNIWARD (JPEG UNIversal WAvelet Relative Distortion) [15], SI-UNIWARD (Side-informed UNIWARD) [15] and so on. Moreover, in literature [16], a new framework for designing distortion functions of JPEG image is proposed by dividing the DCT coefficients into first-priority-group and first-priority-group. The adaptive JPEG steganography constrains the embedding changes to the textured or perceptual complex image regions, and then a higher level of stego-security can be achieved since the embedding noise is covered by the inhered noise. For the above adaptive JPEG steganography algorithms, the steganographic schemes are similar. They all define a distortion function which is related with statistical undetectability firstly and then the messages are embedded by encoding method. For example, as to PQt and PQe, the distortion function is defined according to the texture and energy measure of 8×8 DCT block respectively, and then the given messages are embedded by wet paper code [17]; as to MOD, NPQ, EBS, UED, J-UNIWARD and SI-UNIWARD, the different distortion functions are defined respectively and the messages are embedded while minimizing the distortion function by STCs (Syndrome-Trellis Codes) [18].

For the typical non-adaptive JPEG steganography algorithms, many steganalysis methods have been proposed and achieved high detection accuracies [2]. As to the adaptive JPEG steganographic schemes, different steganalysis methods also have been investigated. In literature [19], the authors pointed out that the distortion function of MOD steganography has been overtrained to an incomplete cover model. Then, a targeted steganalysis method for MOD is proposed by utilizing the statistical features beyond the optimized model. For other adaptive JPEG steganography, the steganographic security is often evaluated by blind steganalysis. For example, in literature [10], the 274-dimensional feature vector consisting of 193 extended DCT features and 81Markov features proposed in [20] is used to detect PQt and PQe. The detection accuracy can only reach to 72% when payload is 0.1bpac (bits per non-zero AC DCT coefficient); in literature [14], the state-of-the-art CC-JRM (Cartesian Calibration JPEG Rich Model) [21] feature is employed to evaluate the security performances of UED steganography and the detection accuracy is about 60% when payload is 0.1bpac and QF (Quality Factor) is 75; in literature [15], the CC-JRM and SRM (Spatial Rich Model) [22]

feature are combined for the detection performance of J-UNIWARD steganography and the detection accuracy is only 55% when payload is 0.1bpac. The steganographic security of SI-UNIWARD is higher than J-UNIWARD because the rounding error of precover image is utilized for the definition of distortion function.

From all above, it can be seen that the detection performance for adaptive JPEG steganography is difficult. This is because the embedding changes are constrained to the complicated image regions which are hard to model. However, the framework of adaptive JPEG steganography make the selection channel of steganography algorithm is public. Furthermore, the stego image is often modified slightly relative to cover image, thus the distortion values of DCT coefficients of stego image will not change or change slightly. Therefore, as to stego image, the steganalyzer can compute the distortion values of DCT coefficients firstly and then the most possibly changed DCT coefficients are selected for the steganalysis feature extraction. In literature [23] and [24], for UNIWARD [15] and WOW [25] steganography which are adaptive steganography in spatial domain, the effects of public selection channel for steganalysis have been discussed. However, for adaptive JPEG steganography, as far as we know, there has no research which pays attention to the public selection channel that would be utilized to improve the detection accuracy. Therefore, in this paper, the effect of selection channel on steganalysis of adaptive JPEG steganography is discussed and a steganalysis method based on DCT coefficient selection is proposed. Firstly, the principle of adaptive JPEG steganography is introduced. Secondly, the practicability of DCT coefficients selection is studied. Next, the proposed steganalysis method is given and the embedding sensitivity of the steganalysis feature extracted from the selected DCT coefficients is analyzed. Lastly, the implement process is presented in details. In the experiments, a series of experiments are implemented to verify the effectiveness of the proposed steganalysis method for some adaptive JPEG steganography algorithms.

2. Adaptive JPEG steganography by minimizing distortion

Let $\mathbf{x}=(x_1,x_2,\cdots,x_n)$ be a cover image and x_i specifies the i th cover element (DCT coefficient). The message is binary bit stream and the corresponding stego image is denoted as $\mathbf{y}=(y_1,y_2,\cdots,y_n)$. The embedding distortion of stego image $\mathbf{y}$ is denoted as $D(\mathbf{y})$, $\pi(\mathbf{y})$ specifies the probability of $\mathbf{x}$ be modified into $\mathbf{y}$. Then, the expected distortion can be expressed as:

$$E_\pi[D]=\sum_{\mathbf{y}\in\mathbf{Y}}\pi(\mathbf{y})D(\mathbf{y}) \tag{1}$$

where $\mathbf{Y}$ denotes the set of all stego images into which $\mathbf{x}$ can be modified.

The minimal distortion adaptive steganography expect to embed a given payload of m bits with minimal possible distortion. The problem is to determine a distribution π that communicates a required payload while minimizing the distortion [18] :

$$\underset{\pi}{\text{minimize}} \quad E_\pi[D]=\sum_{\mathbf{y}\in\mathbf{Y}}\pi(\mathbf{y})D(\mathbf{y}) \tag{2}$$

$$\text{subject to} \quad H(\pi)=m \tag{3}$$

where $H(\pi)=-\sum_{\mathbf{y}\in\mathbf{Y}}\pi(\mathbf{y})\log\pi(\mathbf{y})$ specifies the entropy of the distribution $\pi(\mathbf{y})$.

The optimal distribution π which satisfies Eq. (2) and (3) should has the Gibbs form [26]

$$\pi_\lambda(\mathbf{y}) = \frac{1}{Z(\lambda)}\exp(-\lambda D(\mathbf{y})) \tag{4}$$

where $Z(\lambda)$ is the normalizing factor and parameter $\lambda > 0$.

$$Z(\lambda) = \sum_{\mathbf{y}\in\mathbf{Y}} \exp(\text{-}\lambda \mathrm{D}(\mathbf{y})) \tag{5}$$

When the distortion function $D(\mathbf{y})$ is additive over the cover elements, the distortion caused by embedding changes can be expressed as:

$$D(\mathbf{y}) = \sum_{i=1}^{n} \rho_i(y_i) \tag{6}$$

where $0 \le \rho_i(y_i) \le \infty$ specifies the distortion caused by modifying cover element x_i into stego element y_i. In this case, the embedding changes do not interact and the probability π can be factorized into a product of marginal probabilities of changing the individual cover element.

$$\pi_\lambda(\mathrm{y}) = \prod_{i=1}^{n} \pi_\lambda(y_i) = \prod_{i=1}^{n} \frac{\exp(-\lambda\rho_i(y_i))}{\sum_{y_i\in \mathrm{I}_i}\exp(-\lambda\rho_i(y_i))} \tag{7}$$

where $\pi_\lambda(y_i)$ specifies the probability of x_i be modified into y_i.

Then, the expected distortion and the maximal payload are:

$$E_{\pi_\lambda}[D] = \sum_{i=1}^{n}\sum_{y_i\in \mathrm{I}_i} \pi_\lambda(y_i)\rho_i(y_i) \tag{8}$$

$$H(\pi_\lambda) = -\sum_{i=1}^{n}\sum_{y_i\in \mathrm{I}_i} \pi_\lambda(y_i)\log \pi_\lambda(y_i) \tag{9}$$

In Eq. (7), (8), (9), $I_i = \{x_i, \bar{x}_i\}$ for binary embedding and the bar denotes the operation of flipping the LSB, $I_i = \{x_i - 1, x, x_i + 1\}$ for ternary embedding.

From all above, it can be seen that the adaptive JPEG steganography by minimizing distortion should include distortion function definition and coding method. The former mainly pays attention to measure the distortion caused by embedding changes while the latter should embed the messages and minimize the distortion at the same time. In addition, the cover elements should be modified according to Eq. (7) for simulate embedding [18].

3. Selecting DCT coefficients based on embedding distortion

For adaptive JPEG steganography, the changed DCT coefficients are selected according to the embedding distortion. Let us suppose the embedding changes do not interact, thus the probability of changing the DCT coefficients can be denoted as:

$$p(y) = \frac{\exp(-\lambda\rho(y))}{\sum_y \exp(-\lambda\rho(y))} \tag{10}$$

Furthermore, the partial derivatives of $p(y)$ with respect to distortion ρ is calculated,

$$\frac{\partial p(y)}{\partial \rho} = -\lambda \frac{\exp(-\lambda \rho(y))}{\left(\sum_y \exp(-\lambda \rho(y))\right)^2} \leq 0 \tag{11}$$

In Eq. (11), the parameter $\lambda > 0$ is inverse proportion to embedding payload. Then, from Eq. (11), it can be seen that the changing probability p of DCT coefficient is monotonically decreasing with respect to distortion ρ. In other words, the small embedding distortion means high changing probability while the large embedding distortion means low changing probability. Compared with cover image, the stego image is modified slightly and the distortion values of DCT coefficients will not change or change slightly. Therefore, for the steganalyzers, the distortion values of suspicious image can be calculated firstly and then the most possibly changed DCT coefficients are selected for the steganalysis feature extraction. Next, PQt, PQe and J-UNIWARD steganography are used as examples, the DCT coefficients selection of adaptive JPEG steganography is studied.

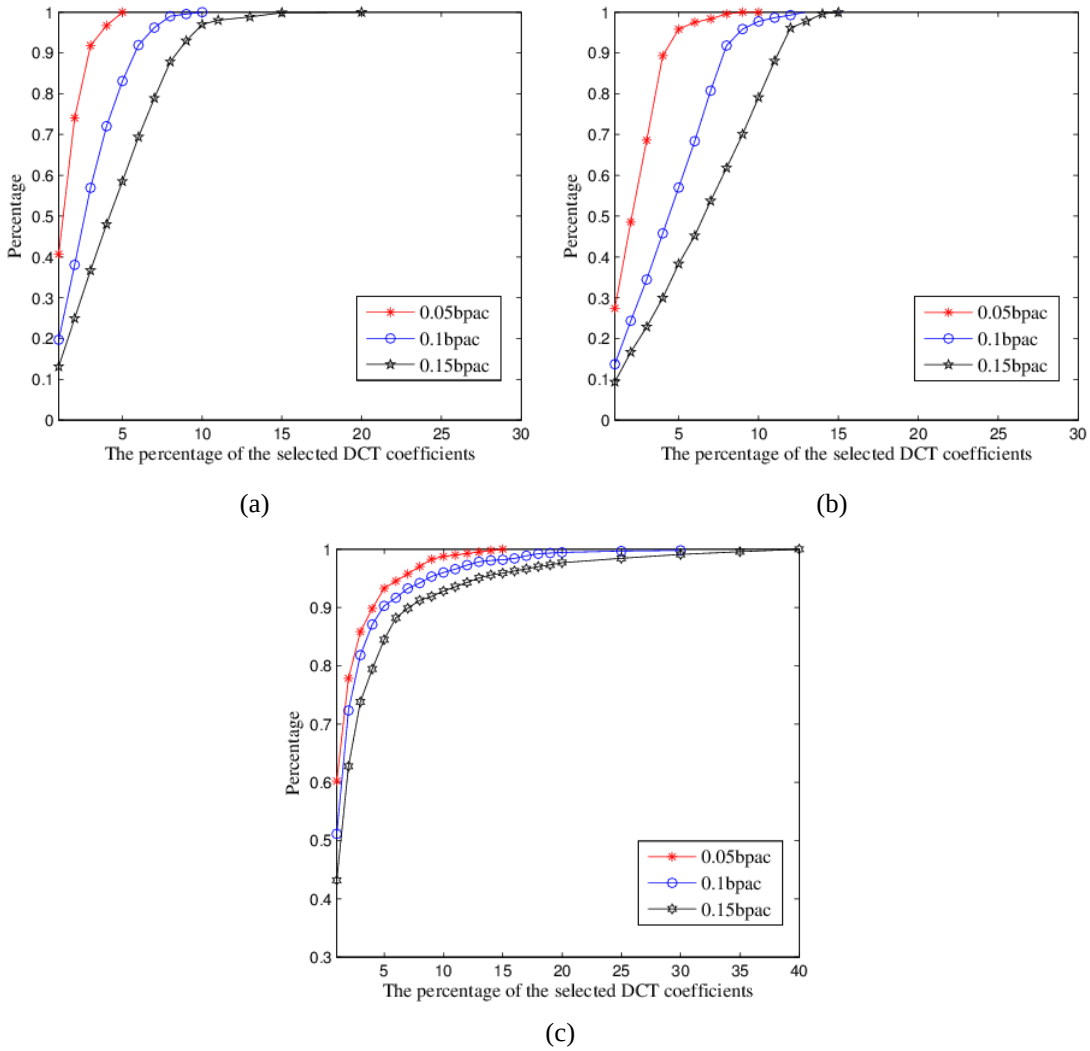

Fig. 1. The percentage of the changed DCT coefficients which have been selected when different percentage DCT coefficients are selected: **(a)** PQt; **(b)** PQe; **(c)** J-UNIWARD.

PQt and PQe belong to the adaptive PQ steganography and the embedding distortions are defined according to the texture and energy measure respectively while J-UNIWARD steganography defines the embedding distortion by image wavelet decomposition coefficients. For these three adaptive JPEG steganography algorithms, the Lena image[1] is used as cover image and the corresponding stego images are generated with different payloads. As to the stego image, the different percentages of DCT coefficients are selected according to embedding distortion from small to large and the percentages of the changed DCT coefficients which have been selected with respect to all the changed DCT coefficients are given.

In **Fig. 1-(a)**, **(b)**, for PQt and PQe, the percentage of the changed DCT coefficients which have been selected are shown when different percentage DCT coefficients are selected according to embedding distortion from small to large. From **Fig. 1-(a)**, **(b)**, it can be seen that the changed DCT coefficients can be got by selecting a small part of the DCT coefficients when the payloads are relative low. In **Fig. 1-(c)**, for J-UNIWARD, the percentages of the changed DCT coefficients are shown when different percentage DCT coefficients are selected. From **Fig. 1-(c)**, it also can be seen that the changed DCT coefficients can be got by selecting a small part of the DCT coefficients when payloads are relatively low.

From the above results, the following conclusions can be drawn for the selection of the changed DCT coefficients.

1) The selection of the changed DCT coefficients according to the embedding distortion is feasible for some adaptive JPEG steganography algorithms. From **Fig.1**, it can be seen that the changed DCT coefficients can be got when only a few DCT coefficients have been selected from Lena image with relatively low payload.

2) The number of the selected DCT coefficients which include all the changed DCT coefficients is much more than the number of the changed DCT coefficients. For PQt and PQe, it is because that the DCT coefficient distortion values for embedding are calculated by the texture and energy measure of the single decompressed JPEG image while the distortion values for DCT coefficients selection are calculated according to the double compressed stego image. Therefore, the distortion values will have some difference and this will affect the selection of DCT coefficients. In addition, steganography embedding also will affect the selection of DCT coefficients. For J-UNIWARD, the DCT coefficients are modified according to the probability given in Eq. (7), thus all the changed DCT coefficients can be got only when more DCT coefficients have been selected.

3) For different adaptive JPEG steganography algorithms, the percentages of the selected DCT coefficients which include all the changed DCT coefficients are different. For example, from **Fig.1-(a)** and **(b)**, it can be seen that the percentages for selecting all the changed DCT coefficients are different for PQt and PQe. This is possible because that the affect caused by double compression and steganography embedding is more for PQe than for PQt. From **Fig.1-(c)**, it can be seen that the percentage is higher for selecting all the changed DCT coefficients. This is because that the embedding changes of J-UNIWARD are implemented according to the probability given in Eq. (7) while the selection of DCT coefficients is according to the distortion values from small to large.

4. Steganalysis method based on DCT coefficients selection

From the above section, it can be seen that the changed DCT coefficients can be selected according to the embedding distortion. Therefore, the steganalyzer can calculate the distortion

[1] Lena image [EB/OL]. http://en.wikipedia.org/wiki/lenna

values of DCT coefficients according to the embedding distortion function firstly, and then extract the steganalysis feature from the selected DCT coefficients with small distortion values. Lastly, the classifier is trained by the steganalysis feature as well as the final steganalyzer. For steganalysis, the same percentage of DCT coefficients is selected, then the steganalysis feature is extracted and the detection is implemented by the trained classifier. In the following, the structure of the proposed steganalysis method is given firstly, then some analyses are presented and the detailed implement processes are described.

4.1 Structure of the proposed steganalysis method

For the steganalysis of adaptive JPEG steganography, the DCT coefficients with small distortion values can be selected for feature extraction and classifier training. However, it should be noticed that the percentage of the selected DCT coefficients varies with payload and the real payload is often unknown for the steganalyzer. Therefore, for a suspicious JPEG image, it is difficult to determine the appropriate percentage of the selected DCT coefficients for feature extraction and steganalysis. In fact, according to the characteristic of adaptive JPEG steganography, we know that it is favorable to the steganalysis of stego image with low payload when the percentage of the selected DCT coefficients is relatively low. On the contrary, the percentage of the selected DCT coefficients should be relatively high for the stego image with high payload.

Thus, the steganalyzer can construct different detector according to the actual demand. In other words, to obtain relatively high detection accuracy for steganography with low payload, relatively few DCT coefficients should be selected to extract steganalysis feature. By contrast, to detect steganography with high payload, much more DCT coefficients should be selected to extracted feature. Furthermore, we can improve the average detection accuracy for adaptive JPEG steganography with different payloads by selecting appropriate percentage of DCT coefficients. Based on the above analysis, a new steganalysis method for adaptive JPEG steganography is proposed, as shown in **Fig. 2**.

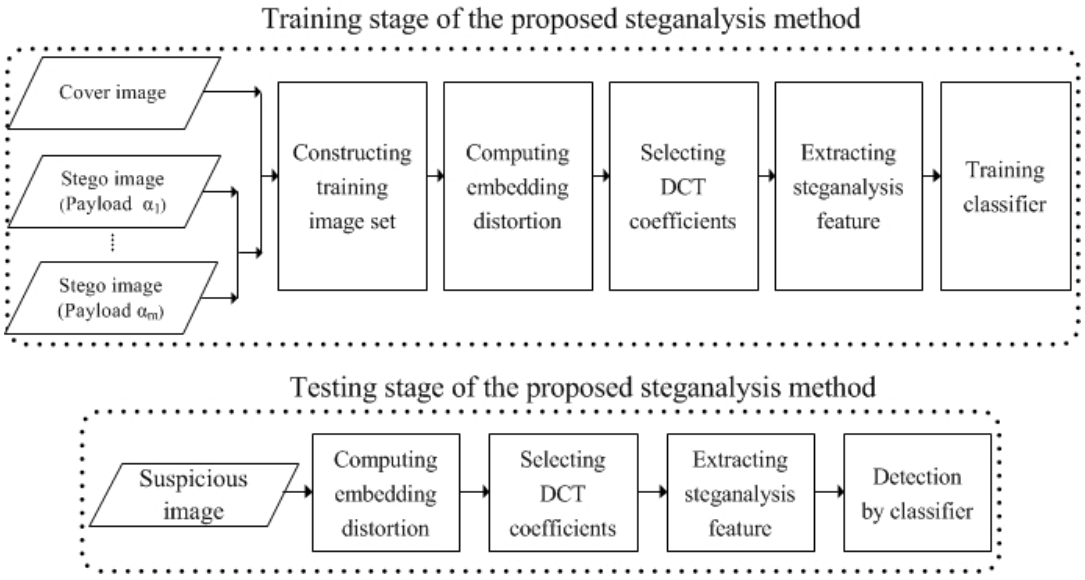

Fig. 2. The structure of the steganalysis method for adaptive JPEG steganography by selecting DCT coefficients.

From the Fig. 2, it can be seen that there are two main stages involved in the proposed steganalysis method by selecting the DCT coefficients, namely, the training stage and the testing stage. In the training stage, the training image set is constructed firstly, which includes the cover images and the corresponding stego images with different payloads from α_1 to α_m. Then, for each training image, the steganalysis feature is extracted from the DCT coefficients which are selected according to the distortion values from small to large. Lastly, the classifier is trained by the extracted steganalysis feature. In the testing stage, for the suspicious image, the same percentage of DCT coefficients is also selected according to the distortion values firstly, and then the steganalysis feature is extracted from these DCT coefficients. Finally, the extracted feature is tested by the trained classifier to obtain the detection result.

4.2 Analysis for the proposed steganalysis method

As shown in **Fig. 2**, the proposed steganalysis method extracts the steganalysis feature from the DCT coefficients which are selected according to the embedding distortion from small to large. The selection of DCT coefficients can increase the change rate of feature extraction source and improve the embedding sensitivity of steganalysis feature.

4.2.1 Change rate of feature extraction source

In **Fig. 3**, the relation between the average change rate and the percentage of the selected DCT coefficients are given for J-UNIWARD steganography with different payloads.

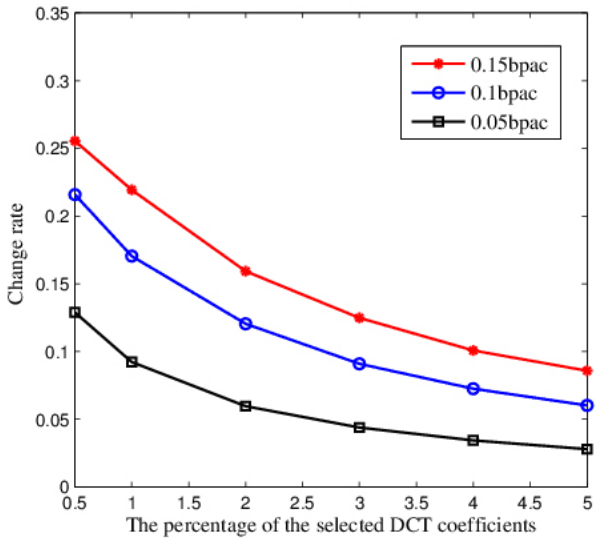

Fig. 3. The relation between change rate and percentage of the selected DCT coefficients.

From **Fig. 3**, it can be seen that the average change rate of the selected DCT coefficients will decrease when more DCT coefficients are selected. Therefore, in contrast to select all the DCT coefficients, the average change rate of feature extraction source can be increased markedly when only partial DCT coefficients with small distortion values are selected.

As we all know, in general, the high change rate of feature extraction source means high embedding sensitivity of steganalysis feature. Therefore, the detection accuracy would be improved by selecting the DCT coefficients according to the embedding distortion. In addition, we should notice that a certain amount of DCT coefficients is necessary for feature extraction even through the change rate will decrease when more much DCT coefficients are selected.

4.2.2 Analysis for embedding sensitivity of steganalysis Feature

For the sensitivity comparison of various features in steganalysis, the rate of the larger value to the smaller value of features before and after embedding is used to measure the sensitivity in [27] and [28]. Suppose a statistical feature before steganography is f, after embedding, it becomes f'. Then, the sensitivity measure value s of it to steganography is:

$$s = \max\left\{\frac{f}{f'}, \frac{f'}{f}\right\} \tag{12}$$

For two types of statistical features f_1 and f_2, after embedding, they are f_1' and f_2' respectively. Denote their sensitivities as s_1 and s_2, respectively. Then, the sensitivity measure values of them to steganography can be calculated using Eq. (12).

For the sensitivity comparison in [27] and [28], they let

$$A = \frac{s_1}{s_2} \tag{13}$$

If $A > 1$, then the feature f_1 is considered superior to f_2, in other words, f_1 is more sensitive to embedding change than f_2, and is more suitable for steganalysis. If $A < 1$, then f_2 is superior to f_1. Otherwise, these two types of features are comparable, i.e., they will get approximately equal accuracy when used for steganalysis.

By the above feature comparision method, the co-occurrence matrix feature extracted from the changed DCT coefficients is compared with the same feature extracted from all the DCT coefficients.

Let the DCT coefficient matrix of a JPEG image be represented with $\mathbf{D} = \left(D_{ij}\right)$, where D_{ij} denotes the (i, j)-th quantized DCT coefficient. Furthermore, let Z denotes the set of the changed DCT coefficients after embedding while P denotes the set of the unchanged DCT coefficients. Then, the set of the adjacent two DCT coefficients along the horizontal direction can be divided into two classes. One is $S_1 = \left\{(D_{ij}, D_{i,j+1}) \mid D_{ij} \in P \text{ and } D_{i,j+1} \in P \right\}$ and the other is $S_2 = \left\{(D_{ij}, D_{i,j+1}) \mid D_{ij} \in Z \text{ or } D_{i,j+1} \in Z \text{ or } D_{ij} \in Z, D_{i,j+1} \in Z\right\}$.

Then, the co-occurrence matrix feature $\mathbf{F}_{All}(a,b)$ and $\mathbf{F}_{Sel}(a,b)$ can be represented as:

$$\mathbf{F}_{All}(a,b) = \frac{C_1(a,b) + C_2(a,b)}{M} \tag{14}$$

$$\mathbf{F}_{sel}(a,b) = \frac{C_2(a,b)}{N} \tag{15}$$

where $C_1(a,b) = \sum_{D_{ij}, D_{i,j+1} \in S_1} \delta(a, D_{i,j}) \delta(b, D_{i,j+1})$, $C_2(a,b) = \sum_{D_{ij}, D_{i,j+1} \in S_2} \delta(a, D_{i,j}) \delta(b, D_{i,j+1})$, $\delta(u,v)$ is a checking function (if and only if $u = v$, $\delta(u,v) = 1$; otherwise, $\delta(u,v) = 0$), $a, b \in [-T, T]$, T denotes the truncation threshold. Moreover, M denotes the number of the elements which belong to the set S_1 and S_2 while N denotes the number of the elements which belong to the set S_2.

According to the sensitivity measure method shown in Eq. (12), the sensitivity measure value of $\mathrm{F}_{All}(a,b)$ and $\mathrm{F}_{Sel}(a,b)$ can be denoted as the follows:

$$s_{All}=\max\left\{\frac{\mathbf{F}_{All}(a,b)}{\mathbf{F}'_{All}(a,b)},\frac{\mathbf{F}'_{All}(a,b)}{\mathbf{F}_{All}(a,b)}\right\} \tag{16}$$

$$s_{Sel}=\max\left\{\frac{\mathbf{F}_{Sel}(a,b)}{\mathbf{F}'_{Sel}(a,b)},\frac{\mathbf{F}'_{Sel}(a,b)}{\mathbf{F}_{Sel}(a,b)}\right\} \tag{17}$$

Furthermore, if suppose $\dfrac{\mathbf{F}_{Sel}(a,b)}{\mathbf{F}'_{Sel}(a,b)}=\dfrac{C_2(a,b)}{C'_2(a,b)}>1$, then,

$$\frac{\mathbf{F}_{All}(a,b)}{\mathbf{F}'_{All}(a,b)}=\frac{C_1(a,b)+C_2(a,b)}{C_1(a,b)+C'_2(a,b)}>1 \tag{18}$$

We can get,

$$\begin{aligned}A&=\frac{\mathbf{F}_{All}(a,b)}{\mathbf{F}'_{All}(a,b)}\cdot\frac{\mathbf{F}'_{Sel}(a,b)}{\mathbf{F}_{Sel}(a,b)}=\frac{C_1(a,b)+C_2(a,b)}{C_1(a,b)+C'_2(a,b)}\cdot\frac{C'_2(a,b)}{C_2(a,b)}\\&=\frac{C_1(a,b)\cdot C'_2(a,b)+C_2(a,b)\cdot C'_2(a,b)}{C_1(a,b)\cdot C_2(a,b)+C'_2(a,b)\cdot C_2(a,b)}<1\end{aligned} \tag{19}$$

So, the feature $\mathbf{F}_{Sel}(a,b)$ is more sensitive to embedding changes than $\mathbf{F}_{All}(a,b)$.

Similarly, if suppose $\dfrac{\mathbf{F}_{Sel}(a,b)}{\mathbf{F}'_{Sel}(a,b)}=\dfrac{C_2(a,b)}{C'_2(a,b)}<1$, we also can get the feature $\mathbf{F}_{Sel}(a,b)$ is more sensitive than the feature $\mathbf{F}_{All}(a,b)$.

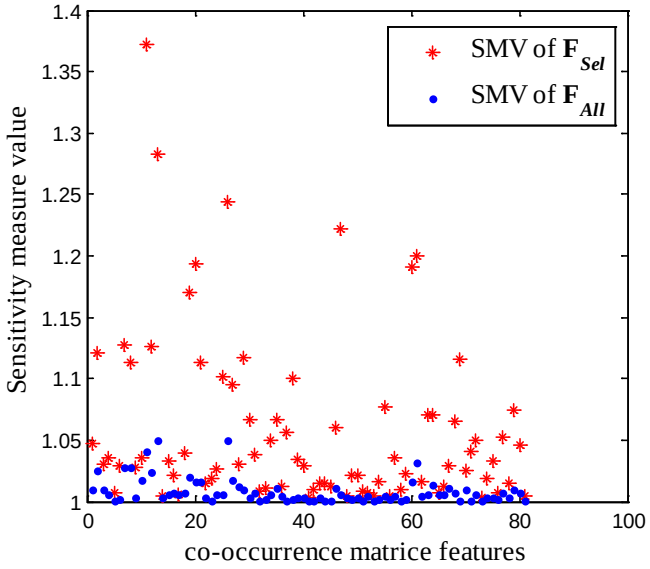

Fig. 4. Comparison for the sensitivity measure values of the steganalysis feature F_{Sel} and F_{All}.

From the above analysis, it can be seen that the co-occurrence matrix feature extracted from the changed DCT coefficients is more sensitive to embedding than the same feature extracted from all the DCT coefficients. For the other steganalysis feature, the similar analyses can be

implemented. Noticed that, even through we can not select the changed DCT coefficients alone, the embedding sensitivity of the steganalysis feature extracted from the selected DCT coefficients also would be better. In **Fig. 4,** for PQt steganography with payload 0.05bpac, the sensitivity measure value (SMV) of the steganalysis feature F_{All} and F_{Sel} is given. Here, the feature F_{Sel} is extracted from the selected DCT coefficients (the percentage is 5%) and the threshold $T = 4$. So, the parameters $a, b \in [-4,4]$ and the feature dimension is 81. From **Fig. 4**, it can be seen that the steganalysis feature F_{Sel} is more sensitive to F_{All}.

4.3 Implement processes of the proposed steganalysis method

The detailed implement processes can be described as the following:

Step1: Constructing the training image set

The training image set is formed by cover images and stego images. One cover image and the corresponding stego image with certain payload is a training sample pair. All the training sample pairs are used for feature extraction.

Step2: Extracting the steganalysis feature

For each image of the training samples, the following processes are implemented:

1) The distortion values of all the DCT coefficients of the sample image are computed according to the distortion function of adaptive JPEG steganography algorithm;

2) The DCT coefficients are sorted according to the distortion values from small to large;

3) A given percentage of DCT coefficients are selected from the DCT coefficients with the smallest distortion;

4) The steganalysis feature is extracted from the selected DCT coefficients.

Step3: Training the classifier

After the steganalysis features have been extracted, the classifier is trained as the final steganalyzer. It should be noticed that different classifiers should be trained for different detection performance. For example, as to J-UNIWARD steganography with payload 0.1bpac, the training image set should only include the cover image and the corresponding stego image with payload 0.1bpac, and then the classifier is trained by the feature extracted from the selected DCT coefficients with certain percentage. Moreover, for different steganography and payload, the training set and classifier are all different.

Step4: Steganalysis

In the steganalysis stage, for the suspicious image, the same percentage of DCT coefficients are selected according to the distortion values from small to large firstly, and then the steganalysis feature is extracted from these DCT coefficients. Finally, the extracted feature is tested by the trained classifier to obtain the detection result.

For the proposed method, the DCT coefficients for feature extraction are selected according to the embedding distortion function. Therefore, in contrast to blind steganalysis, the proposed method belongs to the targeted steganalysis in some sense. In addition, for a suspicious image, the payload is often unknown and we can not determine the optimal percentage parameter for the selection of DCT coefficients. However, we can improve the average detection accuracy for adaptive JPEG steganography with payload in a given range by selecting appropriate percentage of DCT coefficients. That is to say, the payload of a suspicious image is not needed. Certainly, we can get better detection performance if the payload of the suspicious image can be got. However, estimating the payload is rather difficult especially for modern schemes whose detection requires high-dimensional statistical features.

5. Experimental results and analysis

5.1 Image Database and Experiment setup

In the experiments, the original images are from BossBase-1.01 [29]. For PQt and PQe, all these grayscale images are converted into JPEG image with QF 85, and then stego images are generated with payload 0.05, 0.1, 0.15, 0.2, 0.3, 0.4, and 0.5bpac (bits per non-zero AC DCT coefficient) respectively, the QF of double-compression is 70. For J-UNIWARD, all these original grayscale images are converted into JPEG image with QF 75. Then, the stego images are generated with the same seven payloads. In all experiments, ensemble classifier [30] is used for the training and testing. The proportion of training set to test set is 7:3, the detection accuracy is defined as $(P_{TP}+P_{TN})/2$, P_{TP}, P_{TN} denotes the probability of true positive and true negative respectively. The final detection accuracy is the average value of ten duplicate experiments. In subsection 5.4, for each steganography algorithm, the training set contains 7000 cover images and corresponding stego images with different payloads. The testing set contains the remaining 3000 cover images and corresponding stego images. The proportion of stego images with different payloads is same for the training and testing set.

5.2 Effect of selecting possibly changed DCT coefficients

In the section, CC-JRM [21] feature extracted from the selected DCT coefficients is utilized to detect the adaptive JPEG steganography PQt, PQe and J-UNIWARD with certain payload.

5.2.1 Steganalysis of PQt and PQe steganography

As to PQt, the embedding distortion is defined according to the texture measure of DCT blocks. So the given percentage of DCT coefficients should be selected from the highest texture measure to the lowest texture measure. Furthermore, CC-JRM is extracted from these selected DCT coefficients and used to detect PQt. The relations between the detection accuracies and the percentages of the selected DCT coefficients are shown in **Table 1**.

Table 1. Detection accuracies for PQt when different percentages of DCT coefficients are selected

Payload	2%	3%	4%	5%	6%	8%	10%	12%	20%	25%	100%
0.05	72.61	**74.94**	72.83	70.83	70.11	69.06	66.39	65.83	64.15	63.83	62.11
0.10	72.39	80.00	83.00	**83.50**	83.44	81.89	80.06	78.61	78.39	75.33	73.78
0.15	73.48	81.11	85.28	86.56	**88.61**	88.06	88.00	87.00	84.17	84.17	82.89
0.20	73.50	81.33	86.28	88.83	91.22	91.50	**91.94**	91.83	89.94	89.89	88.06
0.30	73.56	81.38	86.44	88.89	91.56	92.06	94.06	95.33	**95.43**	94.72	94.11
0.40	73.94	81.56	86.63	89.61	91.72	92.44	95.17	95.67	96.33	**96.89**	96.72
0.50	73.96	81.78	86.94	89.72	91.76	92.94	95.41	95.78	97.28	**97.56**	97.50

From the experimental results in **Table 1**, it can be seen that the detection accuracy for PQt will be improved by selecting the DCT coefficients. Moreover, the improvement is quite obvious when payload is relatively low.

For PQe, the embedding distortion is defined according to the energy measure of DCT blocks. So the given percentage of DCT coefficients should be selected from the highest

energy measure to the lowest energy measure. Then, CC-JRM is extracted from these selected DCT coefficients. The detection performances for PQe steganography are shown in **Table 2**.

Table 2. Detection accuracies for PQe when different percentages of DCT coefficients are selected

Payload	5%	6%	7%	8%	10%	12%	20%	25%	30%	35%	100%
0.05	76.83	**78.78**	77.94	77.83	76.33	75.39	70.33	68.33	66.17	65.17	62.60
0.10	79.78	82.28	84.56	85.22	85.28	**86.39**	83.56	80.78	78.28	75.61	73.06
0.15	80.11	83.12	85.33	87.17	88.11	**90.22**	89.78	88.72	86.77	85.11	81.33
0.20	81.44	83.44	85.72	88.11	88.33	90.78	**93.33**	92.28	91.44	90.44	86.56
0.30	81.89	83.83	85.78	88.12	89.17	91.44	94.61	**96.07**	95.67	95.61	93.28
0.40	82.36	84.22	86.83	88.28	89.50	91.89	94.83	96.28	96.78	**97.00**	95.61
0.50	82.42	84.72	86.94	88.48	89.72	92.10	95.17	96.61	97.17	**98.17**	97.50

From the experimental results in **Table 2**, it can be seen that the detection accuracy for PQe also can be improved by extracting feature from the selected DCT coefficients. Contrast to PQt, more DCT coefficients should be selected in order to obtain the high detection accuracy for the same payload. This is because the changed DCT coefficients can be got only when more DCT coefficients have been selected (as shown in **Fig. 1-(a)** and **(b)**).

5.2.2 Steganalysis of J-UNIWARD steganography

For J-UNIWARD, the relations between the detection accuracies and the percentages of the selected DCT coefficients with respect to all DCT coefficients are shown in **Table 3**.

Table 3. Detection accuracies for J-UNIWARD when different percentages of DCT coefficients are selected

Payload	5%	10%	15%	20%	25%	30%	35%	40%	45%	50%	100%
0.05	64.50	65.72	**68.72**	67.52	67.06	66.76	66.50	66.44	65.39	65.11	50.61
0.10	68.89	69.44	72.67	**73.67**	71.83	71.61	69.61	69.39	68.83	68.06	52.17
0.15	69.06	72.67	72.77	73.72	**74.50**	72.33	71.56	70.56	70.33	69.61	54.78
0.20	69.26	75.11	75.50	75.63	**75.79**	73.72	72.50	72.00	71.72	70.67	56.78
0.30	69.44	75.44	77.39	77.67	78.28	**78.67**	75.94	75.56	74.72	74.06	64.39
0.40	69.47	77.17	79.11	79.72	80.22	80.28	**80.78**	79.83	78.22	78.00	73.28
0.50	69.58	78.89	81.28	82.28	82.78	83.33	84.50	**84.78**	82.78	82.78	80.00

From the experimental results in **Table 3**, it can be seen that the detection accuracies for J-UNIWARD also can be improved by selecting the DCT coefficients.

5.3 Detection performances of different steganalysis features

In this part, the CC-PEV [31], CC-CHEN [32] and CC-JRM features extracted from the selected DCT coefficients are compared with the same features extracted from all the DCT coefficients for the steganalysis of PQt, PQe and J-UNIWARD.

In **Table 4**, the detection performances with different features are compared for PQt. The features CC-PEV-S, CC-CHEN-S and CC-JRM-S denote the three typical steganalysis features extracted from the selected DCT coefficients according to the embedding distortion.

Table 4. Detection performances for PQt with different features

Payload	CC-PEV	CC-PEV-S	CC-CHEN	CC-CHEN-S	CC-JRM	CC-JRM-S
0.05	54.17	66.67	54.22	64.33	62.11	74.94
0.10	61.78	74.17	60.17	69.67	73.78	83.50
0.15	68.17	77.78	66.00	74.89	82.89	88.61
0.20	72.78	82.50	71.56	77.50	88.06	91.94
0.30	82.83	87.44	80.72	83.44	94.11	95.43
0.40	90.17	90.83	86.61	85.50	96.72	96.89
0.50	94.94	93.44	90.83	87.67	97.50	97.56

From **Table 4**, it can be seen that the detection accuracy can be improved only if the features are extracted from the selected DCT coefficients. For example, when payload is 0.05bpac, the detection accuracy of CC-PEV, CC-CHEN and CC-JRM is 54.17%, 54.22%, and 62.11% while the detection accuracy of the corresponding features extracted from the selected DCT coefficients is 66.67%, 64.33%, and 74.94%.

The detection performances for PQe with different features are shown in **Table 5**. From **Table 5**, it also can be found that the detection accuracy for PQe can be improved by extracting feature from the selected DCT coefficients. This is particularly obvious when the payload is relative low.

Table 5. Detection performances for PQe with different features

Payload	CC-PEV	CC-PEV-S	CC-CHEN	CC-CHEN-S	CC-JRM	CC-JRM-S
0.05	57.72	73.56	57.22	66.94	62.60	78.78
0.10	65.83	79.67	62.39	72.17	73.06	86.39
0.15	72.28	81.83	67.33	75.89	81.33	90.22
0.20	77.83	84.94	71.83	78.44	86.56	93.33
0.30	85.39	89.50	80.61	82.33	93.28	96.07
0.40	91.50	92.56	85.67	86.50	95.61	97.00
0.50	94.67	93.89	89.78	87.50	97.50	98.17

The detection performances for J-UNIWARD are shown in **Table 6**. From **Table 6**, it can be seen that the detection accuracies of CC-PEV, CC-CHEN and CC-JRM are poor when payload is low. However, if the same features are extract from the selected DCT coefficients, the detect accuracy can be improved greatly. For example, when payload is 0.05bpac, the detection accuracy of the three original features is only 50%, 50.33%, and 50.61% while it can reach 65.00%, 59.00% and 68.72% if the same features are extracted from the selected DCT coefficients.

Table 6. Detection performances for J-UNIWARD with different features

Payload	CC-PEV	CC-PEV-S	CC-CHEN	CC-CHEN-S	CC-JRM	CC-JRM-S
0.05	50.00	65.00	50.33	59.00	50.61	68.72
0.10	52.56	66.83	50.50	60.00	52.17	73.67
0.15	54.11	70.17	51.11	61.23	54.78	74.50
0.20	56.17	71.15	55.00	65.00	56.78	75.79
0.30	62.61	72.67	59.89	69.33	64.39	78.67
0.40	69.11	74.67	66.44	74.17	73.28	80.78
0.50	76.17	76.39	74.83	76.33	80.00	84.78

5.4 Detection performances of the proposed steganalysis method

For real steganalysis, the payload is often unknown, and the appropriate percentage of the selected DCT coefficients is difficult to be determined for steganalysis feature extraction. However, we can construct different detector to meet the demand. For example, if we want to make good average detection accuracy for PQt steganography with payload from 0.05bpac to 0.5bpac, we should extract the feature from cover images and the corresponding stego images by selecting the appropriate percentage of DCT coefficients. Then, classifier is trained by the extracted feature to get the detector for PQt steganography. In **Table 7**, the detection accuracies of CC-JRM-S extracted from different percentages of DCT coefficients are given for PQt steganography with payload from 0.05bpac to 0.5bpac.

Table 7. Detection accuracies of CC-JRM-S extracted from different percentage of DCT coefficients

Payload	3%	4%	5%	6%	8%	10%	12%
0.05	74.50	72.44	68.33	64.00	61.03	58.55	56.50
0.10	80.50	83.83	82.72	81.50	80.27	76.83	75.00
0.15	81.28	86.39	87.00	87.72	87.12	86.55	85.38
0.20	81.44	86.61	88.38	89.66	90.83	91.11	91.94
0.30	81.72	86.94	88.83	89.77	90.94	92.22	93.05
0.40	81.77	87.00	88.88	90.00	91.05	92.22	93.41
0.50	81.83	87.16	88.89	90.27	91.16	92.23	93.50
Average accuracy	80.43	84.33	**84.71**	84.70	84.62	84.24	84.11

From **Table 7**, it can be seen that the average detection accuracy is best for PQt steganography with 0.05 to 0.5bpac when 5% DCT coefficients are selected. Similarly, the detector can be constructed for other demand. The difference lies in the construction of the training set and the percentage of the selected DCT coefficients. For example, if we want to make good average detection accuracy for PQt steganography whose payloads are from 0.1 to 0.5bpac. Then, the training set should include the cover images and the corresponding stego images whose payloads are from 0.1bpac to 0.5bpac. Furthermore, the percentage of the selected DCT coefficients for feature extraction will be high.

In the following, the steganalysis method by selecting DCT coefficients (SBSD) is compared with the steganalysis method based on all the DCT coefficients (SBAD). In the experiments, the CC-JRM-S is used for steganalysis. The detection accuracies of the two steganalysis method for PQt, PQe and J-UNIWARD are shown in **Table 8-10**, the symbols '—' denotes the stego images with the corresponding payload are not used for training and testing. The "5%", "6%" and so on in **Table 8-10** specify the percentage of the selected DCT coefficients with respect to all the DCT coefficients of JPEG image.

Table 8. Performance comparisons for steganalysis of PQt based on SBAD and SBSD

Method	0.05	0.1	0.15	0.2	0.3	0.4	0.5	Average accuracy
SBAD	55.50	65.38	75.88	84.94	92.16	92.88	93.16	79.98
SBSD (5%)	68.33	82.72	87.00	88.38	88.83	88.88	88.89	**84.71**
SBAD	—	62.83	74.05	85.05	93.44	94.16	94.33	83.97
SBSD (6%)	—	79.05	87.77	91.66	91.94	91.77	91.33	**88.92**
SBAD	—	—	71.61	82.72	94.16	95.44	95.77	87.94
SBSD (10%)	—	—	85.61	91.22	93.27	93.50	93.22	**91.36**
SBAD	—	—	—	76.33	93.27	95.55	95.94	90.27
SBSD (12%)	—	—	—	91.61	95.50	96.27	96.28	**94.91**
SBAD	—	—	—	—	91.22	96.50	97.44	95.05
SBSD (15%)	—	—	—	—	95.38	97.55	97.72	**96.88**
SBAD	—	—	—	—	—	96.61	98.11	97.36
SBSD (20%)	—	—	—	—	—	97.00	98.27	**97.63**

Table 9. Performance comparisons for steganalysis of PQe based on SBAD and SBSD

Method	0.05	0.1	0.15	0.2	0.3	0.4	0.5	Average accuracy
SBAD	58.38	68.44	76.05	83.22	89.66	91.22	91.72	79.81
SBSD (8%)	74.88	83.33	85.50	85.83	86.00	85.61	86.11	**83.89**
SBAD	—	66.61	75.61	83.72	90.66	92.50	93.16	83.71
SBSD (12%)	—	84.61	88.88	90.11	90.44	90.61	90.38	**89.17**
SBAD	—	—	73.83	82.27	91.05	93.44	94.11	86.94
SBSD (20%)	—	—	87.72	91.22	93.00	93.16	93.22	**91.66**
SBAD	—	—	—	79.61	91.33	94.55	95.22	90.17
SBSD (25%)	—	—	—	90.61	94.61	95.33	95.38	**93.98**
SBAD	—	—	—	—	90.05	95.44	96.55	94.01
SBSD (30%)	—	—	—	—	94.61	96.72	97.16	**96.16**
SBAD	—	—	—	—	—	95.38	97.00	96.19
SBSD (35%)	—	—	—	—	—	96.66	97.22	**96.94**

Table 10. Performance comparisons for steganalysis of J-UNIWARD based on SBAD and SBSD

Method	0.05	0.1	0.15	0.2	0.3	0.4	0.5	Average accuracy
SBSD	51.44	52.88	56.00	59.38	65.55	72.44	76.05	61.96
SBSD (15%)	58.61	67.11	70.77	73.00	73.22	73.42	73.55	**69.95**
SBAD	—	52.83	55.44	58.44	65.66	72.11	76.22	63.45
SBSD (20%)	—	66.38	71.22	74.22	77.00	77.16	77.36	**73.89**
SBAD	—	—	55.11	59.05	66.55	73.55	78.00	66.45
SBSD (25%)	—	—	69.44	74.27	77.66	79.05	80.05	**76.09**
SBAD	—	—	—	58.11	65.44	72.61	78.05	68.55
SBSD (30%)	—	—	—	70.94	76.94	79.61	82.44	**77.48**
SBAD	—	—	—	—	65.05	73.72	79.72	72.83
SBSD (35%)	—	—	—	—	74.83	80.16	83.16	**79.38**
SBAD	—	—	—	—	—	73.05	80.27	76.66
SBSD (40%)	—	—	—	—	—	79.94	84.44	**82.19**

From **Table 8**, it can be seen that the average detection accuracy of SBSD is 84.71% when the payloads of stego images are from 0.05 to 0.5bpac. The average detection accuracy can reach 97.63% when the payloads are from 0.4 to 0.5bpac. For the same payloads, the average detection accuracies of SBAD are 79.98% and 97.36% respectively. In other words, the SBSD can achieve better average detection accuracy than the SBAD. Especially, contrast to SBAD, the SBSD can make much better detection accuracy for PQt with low payload. For example, for PQt with payload 0.05bpac, the detection accuracy of SBSD is 68.33% while it is only 55.50% achieved by SBAD.

From **Table 9**, it can be seen that the SBSD also can improve the average detection accuracy for PQe. In addition, for the PQe steganography with low payload, the improvement of detection accuracy is more obvious. For example, for PQe with payload 0.05bpac, the detection accuracy of SBSD is 74.88% while it is only 58.38% achieved by SBAD.

From **Table 10**, it can be seen that the SBSD also can improve the average detection accuracy for J-UNIWARD. As to the low payload, the improvement is more obvious. For example, for J-UNIWARD with payload 0.1bpac, the detection accuracy of SBSD is 67.11% while it is only 52.88% achieved by SBAD.

From all above it can be found that the SBSD method can improve the average detection accuracy for PQt, PQe and J-UNIWARD. When payload is low, the improvement is quite obvious. Notice that, for PQt, when less DCT coefficients are selected for feature extraction, the detection accuracy for high payload such as 0.3, 0.4, 0.5bpac will decrease possibly even if the average accuracy will be improved. It is similar for PQe and J-UNIWARD. However, in actual application, the payload is often relatively low, so the proposed steganalysis method is appropriate for PQt, PQe and J-UNIWARD.

6. Conclusions

In this paper, a steganalysis method by selecting the possibly changed DCT coefficients is proposed to enhance the sensitivity of steganalysis feature and improve the detection accuracy.

The experimental results show the proposed method can improve the average detection accuracy for the three adaptive JPEG steganography with different payloads. Especially, the improvements are obvious for low payloads. For other adaptive JPEG steganography, such as UED, the changed DCT coefficients are relatively large when the payload is low. Therefore the detection accuracy only will be improved slightly because the embedding changes of large DCT coefficients can not be captured effectively by the existing feature. As to NPQ**,** EBS and SI-UNIWARD, the changed DCT coefficients are relatively scattered and are difficult to be selected accurately because the rounding error of precover is unknown for steganalyzer, so the improvement is also not obvious by selecting DCT coefficients. In the future, the new steganalysis method should be developed for these adaptive JPEG steganography.

References

[1] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol.90, no.3, pp.727–752, March, 2010. Article (CrossRef Link).

[2] X.Y. Luo, D. S. Wang, P. Wang, and F. L. Liu, "A review on blind detection for image steganography," *Signal Processing*, vol.88, no.9, pp.2138–2157, September, 2010. Article (CrossRef Link).

[3] D. Upham, "Steganographic algorithm Jsteg," Software available at Article (CrossRef Link).

[4] P. Sallee, "Model-based steganography," in *Proc. of 2nd Int. Workshop Digital Watermarking*, pp. 154–167, October 20-22, 2003. Article (CrossRef Link).

[5] P. Sallee, "Model-based methods for steganography and steganalysis," *International Journal of Image Graphics*, vol.5, no.1, pp.167–190, January, 2005. Article (CrossRef Link).

[6] N. Provos, "Defending against statistical steganalysis," in *Proc. of 10th Usenix Security Symposium*, pp. 323–335, August 13-17, 2001. Article (CrossRef Link).

[7] A. Westfeld, "High capacity despite better steganalysis (F5–A steganographic algorithm)," in *Proc. of 4th Int. Workshop on Information Hiding*, pp. 289–302, April 25-27, 2001. Article (CrossRef Link).

[8] J. Fridrich, M. Goljan, and D. Soukal, "Perturbed Quantization Steganography," *ACM Multimedia System Journal*, vol.11, no.2, pp.98-107, February, 2005. Article (CrossRef Link).

[9] Y. Kim, Z. Duric, and D. Richards, "Modified matrix encoding technique for minimal distortion steganography," in *Proc. of 8th Int. Workshop Information Hiding*, pp. 314–327, July 10-12, 2006. Article (CrossRef Link).

[10] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities", in *Proc. of 9th ACM Multimedia and Security Workshop*, pp. 3–14, September 20-21, 2007. Article (CrossRef Link).

[11] T. Filler and J. Fridrich, "Design of adaptive steganographic schemes for digital images," in *Proc. of SPIE, Electronic Imaging,Security and Forensics of Multimedia XIII*, volume 7880, pp. OF 1-14, January 23-26, 2011. Article (CrossRef Link).

[12] F. Huang, J. Huang, and Y. Q. Shi, "New Channel Selection Rule for JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol.7, no.4, pp. 1181–1191, April, 2012. Article (CrossRef Link).

[13] C. Wang and J. Q. Ni, "An efficient JPEG steganographic scheme based on the block–entropy of DCT coefficients," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp.1785-1788, March 25-30, 2012. Article (CrossRef Link).

[14] L. J. Guo, J. Q. Ni, and Y.Q. Shi, "An efficient JPEG steganographic scheme using uniform embedding," in *Proc. of 4th IEEE International Workshop on Information Forensics and Security*, pp.169-174, December 2-5, 2012. Article (CrossRef Link).

[15] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. of 1st ACM Information Hiding and Multimedia Security Workshop*, pp.59-68, June 17-19, 2013. Article (CrossRef Link).

[16] F. Huang, W. Luo, J. Huang and Y. Q. Shi, "Distortion Function Designing for JPEG Steganography with Uncompressed Side-image," in *Proc. of 2nd ACM Information Hiding and Multimedia Security Workshop*, pp.69-76, June 17-19, 2013. Article (CrossRef Link).
[17] J. Fridrich, M. Goljan, and D. Soukal, "Wet paper codes with improved embedding efficiency," *IEEE Transactions on Information Forensics and Security*, vol.1, no.1, pp.102–110, January, 2006. Article (CrossRef Link).
[18] 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, March, 2011. Article (CrossRef Link).
[19] J. Kodovský, J. Fridrich, and V. Holub, "On dangers of overtraining steganography to incomplete cover model," in *Proc. of the 13th ACM Multimedia & Security Workshop*, pp. 69–76, September 29-30, 2011. Article (CrossRef Link).
[20] T. Pevný and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG steganalysis," in *Proc. of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, volume 6505, pp. 3 1–3 14, January 29-February 1, 2007. Article (CrossRef Link).
[21] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models," in *Proc. of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XIV*, volume 8303, pp. 0A 1-13, January 22-26, 2012. Article (CrossRef Link).
[22] J. Fridrich, and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol.7, no.3, pp.868–882, March, 2011. Article (CrossRef Link).
[23] T . Denemark, J. Fridrich, and V. Holub, "Further Study on the Security of S-UNIWARD," in *Proc. of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics 2014*, volume 9028, pp. 5 1-5 13, February 3-5, 2014. Article (CrossRef Link).
[24] W. X. Tang, H. D. Li, W. Q. Luo, and J. W. Huang, "Adaptive Steganalysis Against WOW Embedding Algorithm," in *Proc. of the 2nd ACM Workshop on Information Hiding and Multimedia Security*, pp. 91-96, June 11-13, 2014. Article (CrossRef Link).
[25] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters,", in *Proc. of the 4th IEEE International Workshop on Information Forensics and Security*, pp. 234–239, December 2-5, 2012. Article (CrossRef Link).
[26] T. Filler and J. Fridrich, "Gibbs construction in Steganography," *IEEE Transactions on Information Forensics and Security*, vol.5, no.4, pp.705-720, April, 2010. Article (CrossRef Link).
[27] Y. Wang, and P. Moulin, "Optimized feature extraction for learning based image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol.2, no.1, pp.31-45, January, 2007. Article (CrossRef Link).
[28] X. Y. Luo, F. L. Liu, S. G. Lian, and C. F. Yang, "On the typical statistic features for image blind steganalysis," *IEEE Journal on Selected Areas in Communications*, vol.29, no.7, pp.1404-1422 July, 2011. Article (CrossRef Link).
[29] T. Filler, T. Pevný, and P. Bas, "Break Our Steganographic System": The Ins and Outs of Organizing BOSS," in *Proc. of 13th Int. Workshop Information Hiding*, pp. 59–70, May 18-20, 2011. Article (CrossRef Link)
[30] J. Kodovský, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol.7, no.2, pp.432–444, February, 2012. Article (CrossRef Link).
[31] J. Kodovský and J. Fridrich, "Calibration revisited," in *Proc. of 11th ACM Workshop Multimedia and Security*, pp. 63–74, September 7-8, 2009. Article (CrossRef Link).
[32] C. H. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in *Proc. of IEEE International Symposium on Circuits and Systems*, pp. 3029–3032 May 18-21, 2008. Article (CrossRef Link).

Xiaofeng Song received the B.S. degree from the School of Information and Technology, Zhengzhou University, Zhengzhou, China, in 2002, and M.S. degree from the School of Computer Science, Xidian University, Xi'an, China, in 2009. Now, he is a PhD Candidates of the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Science and Technology Institute, China. His current research interest includes steganography, steganalysis and digital image forensic.

Fenlin Liu received the B.S. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 1986, the M.S. degree from Harbin Institute of Technology, Harbin, Heilongjiang, in 1992, and the Ph.D. degree from the Northeast University, Shenyang, Liaoning, in 1998. He is currently a professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, and Zhengzhou Science and Technology Institute. His research interests include information hiding and security theory. He is the author or co-author of more than 100 refereed international journal and conference papers. He obtained the support of the National Natural Science Foundation of China and the Found of Innovation Scientists and Technicians Outstanding Talents of Henan Province.

Chunfang Yang received the M.S. degree and Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2008 and 2012, respectively. Currently, he is a lecturer of Zhengzhou Science and Technology Institute. He is the author or co-author of more than 40 refereed international journal and conference papers. His research interest includes image steganography and steganalysis technique.

Xiangyang Luo received the M.S. degree and the Ph.D. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2004 and 2010, respectively. He is the author or co-author of more than 70 refereed international journal and conference papers. He is currently an associate professor of State Key Laboratory of Mathematical Engineering and Advanced Computing, and Zhengzhou Science and Technology Institute. In addition, he also recently served as guest editor of some special issues of International Journal "Multimedia Tools and Applications" and "International Journal of Internet". His research interest includes multimedia security, image steganography/steganalysis.

Zhenyu Li received the M.S. degree from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2014. Currently, he is a PhD Candidates of Zhengzhou Science and Technology Institute. His research interest includes image steganography and steganalysis technique.