A New Universal Steganalyzer for JPEG Images

Ge Liu[1], Fangjun Huang[2,3](✉), Qi Chen[2], and Zhonghua Li[1]

[1] School of Electronics and Information Technology,
Sun Yat-Sen University, Guangzhou 510006, China
[2] School of Data and Computer Science, Sun Yat-Sen University,
Guangzhou 510006, China
huangfj@mail.sysu.edu.cn
[3] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences,
Beijing 100093, China

Abstract. The JPEG (Joint Photographic Experts Group) file format is currently one of the most widely used image formats. The study on JPEG steganography and steganalysis is a hotspot in the field of information hiding. With the matrix coding and some new adaptive embedding strategies having been put forward, the detection of stego images is becoming more and more difficult. In recent years, a series of new feature extraction methods have been proposed in the field of steganalysis. However, the detection accuracy rate can only be increased by 1–2% points or even less. Based on those existing steganalytic algorithms, a new feature merging method is proposed in this paper. Via merging features extracted from different domains, the detection accuracy rate of those existing JPEG steganalytic algorithms can be improved by 3% points or even higher. Considering about that the feature dimension is so high after feature merging and thus it may bring difficulties in the feature extraction, training and classification process, a new feature selection method is also proposed in this paper. Experimental results demonstrate that it can not only achieve reduction of the dimensionality, but also maintain a high detection accuracy rate.

Keywords: Steganography · Steganalysis · JPEG · Feature merging
Feature selection

1 Introduction

Steganography is a technique for invisible communication. Its purpose is to embed secret messages into digital covers, such as digital images, for covert communication through public communication channels [1]. Conversely, steganalysis is a technique for detecting the presence of hidden messages in cover objects.

Due to the common use of JPEG images in recent years, JPEG image steganography has been proposed one by one, e.g., YASS [2, 3], NPQ [4], DF-US [5], UED [6], UERD [7], J-UNIWARD [8]. Therefore, how to effectively detect the JPEG steganographic algorithms is one of the most urgent practical problems. Currently, researches

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
X. Gu et al. (Eds.): MLICOM 2017, Part I, LNICST 226, pp. 145–157, 2018.
https://doi.org/10.1007/978-3-319-73564-1_15

on steganalysis can be divided into two classes: special steganalysis and universal steganalysis. Special steganalysis [9–11] is designed for a specific hiding technique, while universal steganalysis [12–21] is generally designed for a series of steganographic methods simultaneously. Due to the diversity of the current steganographic techniques, universal steganalysis is more adaptable in practical applications. Accordingly, the universal steganalysis has attracted extensive attention.

The universal steganalysis is based on machine learning and therefore, the key issue is to find distinguishing features that can classify cover images and stego images. This process has two important aspects. The first one is the design of feature extraction. The selected features should react sensitively to the embedding changes but insensitive to the image content. The second one is to propose an effective classifier with low computational complexity. This paper focuses on the first one, namely the design of feature extraction. In terms of feature extraction, it is believed in [13] that the best (most sensitive) features for steganalysis are obtained when they are calculated directly in the embedding domain. Thus, for JPEG images, the features were generally chosen from the quantized discrete cosine transform (DCT) domain for classification in the early study. For example, an effective Markov process (MP) based JPEG steganalysis scheme proposed in [14] utilized both the intrablock and interblock correlations among DCT coefficients; Fridrich et al. extended the 23 DCT features vector [15] to form a 274-dimensional feature vector [16] by merging Markov and DCT features and later, this 274-dimensional feature vector was extended to twice its size by Cartesian calibration [17]; Kodovský et al. extracted a 7850-dimensional feature vector [18] and used a rich model of DCT coefficients to form a 22510-dimensional feature vector [19]. Recently, in addition to extracting features from the DCT domain directly, some new steganalytic methods extracted features from the other domains were also studied. For example, Fridrich extracted a 34671-dimensional feature vector [20] from the spatial domain to attack the JPEG steganographic algorithms. Besides, features can be extracted from the undecimated DCT domain. For example, in [21], Holub et al. introduced a novel feature vector of which features were engineered as first-order statistics of quantized noise residuals obtained from the decompressed JPEG image using 64 kernels of the DCT coefficient matrix (the so-called undecimated DCT). Obviously, the features of these universal steganalyzers above are selected from a single domain, such as the DCT domain, the spatial domain, the undecimated DCT domain.

Based on those existing steganalytic algorithms, a new feature merging method is proposed in this paper. In recent years, though a series of new feature extraction methods have been introduced in the field of steganalysis, the detection accuracy rate can only be increased by 1–2% points or even less compared with those previously proposed methods. In this paper, we firstly propose that those features extracted in different domains can be merged together to form a more powerful steganalyzer, and the experimental results demonstrate the detection accuracy rate can be improved by 3% points or even higher. However, considering about that the feature dimension is so high after feature merging and thus it may bring difficulties to the feature extraction, training and classification, a new feature selection method is also proposed according to some properties introduced in [22]. Our experimental results demonstrate that this new feature selection strategy can not only reduce the dimensionality of the feature vector, but also maintain a high detection accuracy rate.

This paper is organized as follows. In Sect. 2, we present how to merge features extracted from different domains, such as the DCT domain, the spatial domain and the undecimated DCT domain. The new feature selection method is also proposed in Sect. 2. Experiments and results are then given in Sect. 3. Finally, we summarize this paper in Sect. 4.

2 Feature Merging and Feature Selection

2.1 Characteristics of Difference Images in Different Domains

Due to the intrusion characteristics of steganography, some distortion must be introduced to the cover image. In this place, one image randomly selected from BOSSbase ver. 1.01 [23] is exemplified to illustrate the influence of message embedding on the statistical distribution of the JPEG image. First, the image coming from the BOSSbase is compressed with JPEG quality factor (QF) 75, and then used as the cover as shown in Fig. 1(a). The stego image is generated via using the most representative J-UNIWARD JPEG steganographic algorithm [8]. The embedding rate is 0.4 *bpnc* (bits per non-zero DCT coefficients)and the stego image is shown in Fig. 1(b).

(a) (b)

Fig. 1. The cover image and the stego image corresponding to the J-UNIWARD algorithm. (a) The cover image. (b) The stego image with the embedding rate of 0.4 *bpnc*.

Figure 2(a)–(c) illustrate the difference images between the stego image and the cover image in spatial domain, DCT domain, and undecimated DCT domain, respectively. The white points indicate that in these positions the elements (pixels/ coefficients) have been modified, whereas the black points represent in those positions the elements keep untouched in the embedding process. It is observed from Fig. 2 that even if the same steganographic algorithm is applied, the obtained difference images have different statistical distribution characteristics. As we all know, the steganalytic features are extracted to discriminate the difference between the cover and stego images. In general, the features extracted from different domains may complement and reinforce each other. Thus, the detection accuracy rate can be improved via merging features extracted in different domains, such as the DCT domain, the spatial domain, and the undecimated DCT domain.

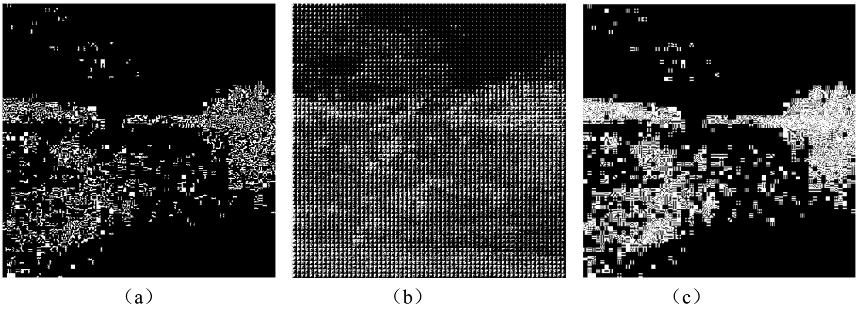
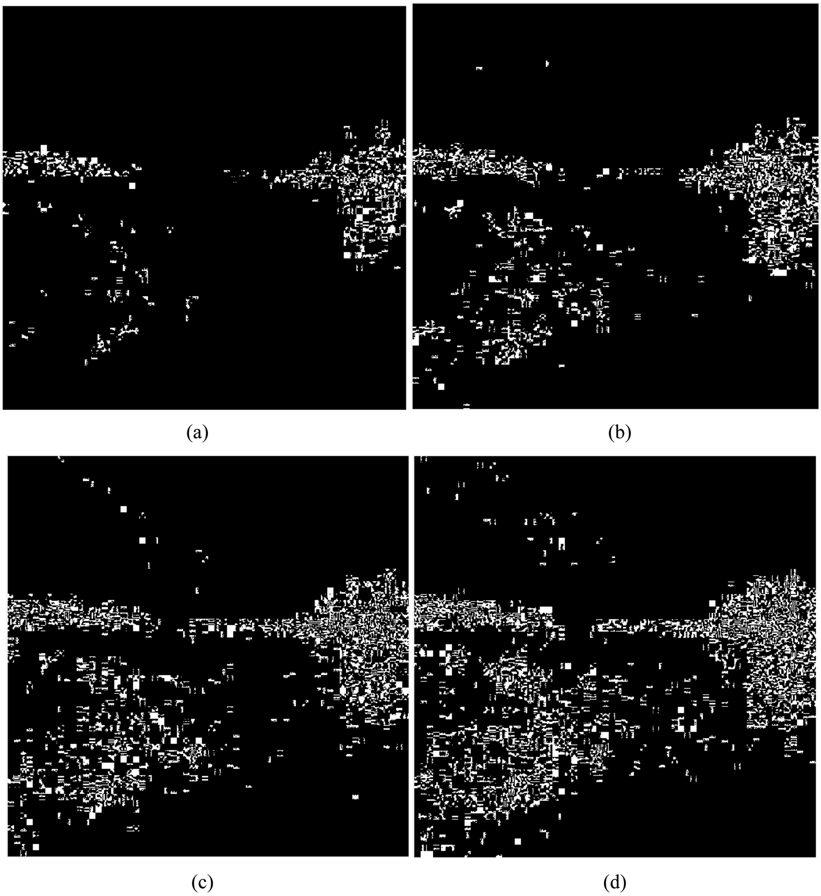


Fig. 2. The difference images between the cover and stego image obtained in different domains with the J-UNIWARD algorithm. (a) The spatial domain. (b) The DCT domain. (c) The undecimated DCT domain.

2.2 Characteristics of Feature Vector

As introduced in our previous work [22], the difference between cover and stego images should consistently increase with the increase of embedding rate. Some experimental results corresponding to the steganographic scheme J-UNIWARD are illustrated in Fig. 3. The cover image is shown in Figs. 1(a) and 3(a)–(d) show the modifications that have been made by using the J-UNIWARD algorithm with different embedding rates.

As seen in Fig. 3, even if embedding rates are different, most of the modifications are made in the same edge areas or complex texture regions. And the difference between cover and stego images will become greater with the increase of embedding rate. As is known, the most basic principle of steganalytic features is to capture the difference between cover and stego images. Via extracting the appropriate features, these two types of images can be classified. In our opinion, if the extracted feature value changes in one direction (consistently decrease or increase) with the increase of embedding rate, this extracted feature should be selected for classification. On the contrary, if the extracted feature presents a randomly decreasing or increasing characteristic, this kind of extracted feature may confuse the classifier and should be excluded from the original feature vector in the steganalytic process. The specific selection method of effective features will be detailed in Sect. 2.3.



(a) (b)

(c) (d)

Fig. 3. Difference images between the cover and stego images regarding to different embedding rates. (a) The difference image with the embedding rate of 0.1 *bpnc*. (b) The difference image with the embedding rate of 0.2 *bpnc*. (c) The difference image with the embedding rate of 0.3 *bpnc*. (d) The difference image with the embedding rate of 0.4 *bpnc*.

2.3 Feature Merging and Feature Selection

Based on the characteristic described in Sects. 2.1 and 2.2, it is obvious that the modifications introduced by embedding messages present different characteristics in different domains and thus steganalysis features in different domains may have different detection ability. The detailed realization of our proposed feature merging method and feature selection method are given in the following.

2.3.1 Merging Features Extracted in Different Domains

Suppose that there are $A_t(t = 1, 2, \ldots)$ feature extracted domains. According to our previous analysis, today's modern steganalytic algorithms generally extract features from one of the domains. Assume that $F_{t,j}(t = 1, 2, \ldots)$ denotes the value of the j^{th}

dimensional feature which is extracted from an image in domain A_t. F_t which denotes the feature vector extracted from the image in domain A_t is defined as

$$F_t = \left\{F_{t,j} | 1 \leq j \leq N_t\right\}, \tag{1}$$

where the parameter N_t denotes the total number of features extracted from an image in domain A_t.

And F which denotes the new feature vector obtained by merging features extracted in different domains is represented as

$$F = [F_1 \, F_2 \ldots]. \tag{2}$$

2.3.2 New Feature Selection Method

Without loss of generality, the merged feature set C extracted from cover image set is defined as

$$C = \left\{C_{i,j} | 1 \leq i \leq M, 1 \leq j \leq N\right\}. \tag{3}$$

And the merged feature set S^{α} extracted from stego images is defined as

$$S^{\alpha} = \left\{S^{\alpha}_{i,j} | 1 \leq i \leq M, 1 \leq j \leq N\right\}. \tag{4}$$

In Eqs. (3) and (4), M denotes the number of images in the image set, N denotes the total number of features after merging features extracted from an image in different domains. The parameter α represents the embedding rate.

Then we can obtain P_j as follows, which denotes mean value of all the j^{th} dimensional features extracted from images in the image set.

$$P_j = \left(\sum\nolimits_{i=1}^{i=M} C_{i,j}\right) / M, \quad (1 \leq j \leq N). \tag{5}$$

And a new variable is defined as

$$T^{\alpha}_j = \sum\nolimits_{i=1}^{M} f\left(S^{\alpha}_{i,j} - P_j\right), \tag{6}$$

where

$$f(x) = \begin{cases} 0, & x \leq 0 \\ 1, & x > 0 \end{cases}. \tag{7}$$

According to our previous analysis in Sect. 2.2, if the value of T^{α}_j in Eq. (6) consistently decreases or increases with the increase of embedding rate α, the j^{th} dimensional feature will be selected as effective feature.

Some experimental results corresponding to the steganalysis scheme JRM are shown in Table 1. We randomly select 5000 images from BOSSbase ver. 1.01, which are compressed as the cover images with QF = 75. Then 5000 stego images are created by using the most representative steganographic algorithm J-UNIWARD with different embedding rates. The cover feature set and stego feature set are extracted from cover and stego images using JRM steganalytic algorithm. We calculate T_j^{α} using Eqs. (5) and (6), where the parameters M and N are equal to 5000 and 22500 respectively. The three $T_j^{\alpha}(j = 6, 11, 19)$ values (i.e., the 6^{th} dimensional feature, the 11^{th} dimensional feature and the 19^{th} dimensional feature) extracted by JRM from 5000 stego images with different embedding rates are shown in Table 1.

Table 1. characteristic of the same feature of difference images with different embedding rates

Embedding rates	T_j^{α} values		
	$j = 6$	$j = 11$	$j = 19$
$\alpha = 0.1bpnc$	2290	2387	2302
$\alpha = 0.2bpnc$	2278	2393	2315
$\alpha = 0.3bpnc$	2275	2368	2325
$\alpha = 0.4bpnc$	2271	2400	2346

It is observed from Table 1 that T_6^{α} corresponding to the 6^{th} dimensional feature (T_{19}^{α} corresponding to the 19^{th} dimensional feature) consistently decrease (increase) with the increase of embedding rate α. Whereas for T_{11}^{α} corresponding to the 11^{th} dimensional feature, it may decrease or increase randomly with the increase of embedding rate α. According to our previous analysis, these kinds of features (e.g., the 6^{th} dimensional feature and 19^{th} dimensional feature) may be effective and should be selected in the steganalytic process. However, those kinds of features (e.g., the 11^{th} dimensional feature) may confuse the classifier and can be excluded from the original feature set in the steganalytic process.

As a result, if T_j^{α} value consistently decreases or increase with the increase of embedding rate α, this extracted j^{th} dimensional feature may be effective and should be selected. Thus, in our proposed method, the extracted feature may be selected as an effective feature in these two cases as follows. Here, a parameter δ is introduced to control the number of selected features.

Case 1: T_j^{α} values consistently decrease with the increase of embedding rate α. The extracted features from the original high dimensional feature set must satisfy the following two conditions.

(1) For any given image set to be tested, the stego images are obtained with different embedding rates, i.e., $\alpha_1, \alpha_2, \ldots, \alpha_n$. For $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_n (n = 1, 2, 3, \ldots)$, if the j^{th} dimensional feature is considered as the effective feature and can be selected for classification, the T_j^{α} values should consistently decrease with the increase of embedding rate α, namely the following inequality (8) must be satisfied, i.e.,

$$T_j^{\alpha_1} > T_j^{\alpha_2} > \cdots > T_j^{\alpha_n} \tag{8}$$

(2) For any given embedding rate, if the j^{th} dimensional $(1 \le j \le N)$ feature is effective, the following inequalities must be satisfied to control the number of selected features.

$$\begin{gathered} 0 \le T_j^{\alpha_1} \le M \times \delta \\ 0 \le T_j^{\alpha_2} \le M \times \delta \\ \vdots \\ 0 \le T_j^{\alpha_n} \le M \times \delta \end{gathered}$$

The parameter δ $(0 < \delta < 1)$ is used to control the number of selected valid classification features. In this paper, we can select $\delta = 0.45$–0.50. Generally, the number of effective features may increase with the increase of δ.

Case 2: T_j^{α} values consistently increase with the increase of embedding rate α. The extracted feature from the original high dimensional feature set must satisfy the following two conditions.

(1) For any given image set to be tested, the stego images are obtained with different embedding rates, i.e., $\alpha_1, \alpha_2, \ldots, \alpha_n$. For $0 < \alpha_1 < \alpha_2 < \cdots < \alpha_n (n = 1, 2, 3, \ldots)$, if the j^{th} dimensional feature is considered as the effective feature and can be selected for classification, the T_j^{α} values should consistently increase with the increase of embedding rate α, namely the following inequality (9) must be satisfied, i.e.,

$$T_j^{\alpha_1} < T_j^{\alpha_2} < \cdots < T_j^{\alpha_n} \tag{9}$$

(2) For any given embedding rate, if the j^{th} dimensional $(1 \le j \le N)$ feature is effective, the following inequalities must be satisfied to control the number of selected features.

$$\begin{gathered} M \times (1 - \delta) \le T_j^{\alpha_1} \le M \\ M \times (1 - \delta) \le T_j^{\alpha_2} \le M \\ \vdots \\ M \times (1 - \delta) \le T_j^{\alpha_n} \le M \end{gathered}$$

Similarly, we can select $\delta = 0.45$–0.50.

3 Experimental Results

3.1 Experiment Setup

In this paper, we utilize the BOSSbase ver. 1.01 [23] image data set for all of our experiments. It consists of 10000 gray-scale images with the size 512 × 512, which are compressed as the cover images with QF = 75. The stego images are generated by using the most representative JPEG steganographic algorithm J-UNIWARD with different embedding rates. Four different embedding rates, i.e., 0.1 *bpnc*, 0.2 *bpnc*, 0.3 *bpnc* and 0.4 *bpnc*, are selected in our testing. The ensemble classifier [18] is used for classification. We randomly select 5000 images for training and the remaining 5000 images are used for testing.

3.2 Experiment #1

In this experiment, algorithm SRM [20] is applied to extract features from JPEG stego images in A_1 domain (the spatial domain). The dimension of the SRM feature vector is $N_1(N_1 = 34671)$. Algorithm JRM [19] is applied to extract features from JPEG stego images in A_2 domain (the DCT domain). The dimension of the JRM feature vector is $N_2(N_2 = 22510)$. Algorithm DCTR [21] is applied to extract features from JPEG stego images in A_3 domain (the undecimated DCT domain). The dimension of the DCTR feature vector is $N_3(N_3 = 8000)$. A new feature vector is obtained by merging features extracted in two or three different domains. The ensemble classifier [18] is used for classifying JPEG cover images and JPEG stego images. The efficiency of our proposed feature merging method is shown in the Table 3. In comparison, the efficiency of the features extracted in a single domain is shown in the Table 2. In this case, three different steganalysis schemes, i.e., SRM, JRM and DCTR and four different embedding rates, i.e., 0.1 *bpnc*, 0.2 *bpnc*, 0.3 *bpnc*, 0.4 *bpnc* are tested.

Table 2. Features dimension and testing error for four different embedding rates in different single domain

Embedding rates (*bpnc*)	Testing error		
	SRM	JRM	DCTR
Dimension	34671	22510	8000
0.1	0.4514	0.4725	0.4383
0.2	0.3797	0.4177	0.3408
0.3	0.2857	0.3411	0.2368
0.4	0.1988	0.2585	0.1504

From the Tables 2 and 3, it is obvious that the detection accuracy rate can be improved via merging features extracted from different domains. For example, when the embedding rate is 0.4 *bpnc*, the testing error of the steganalysis scheme SRM is

Table 3. Features dimension and testing error of merging features

Embedding rates (*bpnc*)	Testing error			
	SRM + JRM	SRM + DCTR	JRM + DCTR	SRM + JRM + DCTR
Dimension	57181	42671	30510	65181
0.1	0.4464	0.4445	0.4385	0.4385
0.2	0.3585	0.3395	0.3370	0.3378
0.3	0.2664	0.2344	0.2309	0.2214
0.4	0.1667	0.1397	0.1402	0.1320

0.1988 with the feature dimension of 34671, while the testing error of the steganalysis scheme JRM is 0.2585 with the feature dimension of 22510, and the testing error of the steganalysis scheme DCTR is 0.1504 with the feature dimension of 8000. However, when combines SRM features and JRM features together, the testing error works out to be 0.1667 with the feature dimension of 57181. This indicates that the new feature merging method achieves to a higher classification rate by 3% points or even higher compared to the JPEG steganalytic algorithms SRM and JRM. Furthermore, when combines the SRM features, JRM features and DCTR features simultaneously, the testing error can be decreased to 0.1352 with the feature dimension of 65181. That is to say, its detection accuracy rate can be improved by 2–3% points or even more.

3.3 Experiment #2

Based on experiment 1 presented in Sect. 3.2, this experiment is to demonstrate the efficiency of our new method for dimensionality reduction, and the results are shown in Table 4. In this experiment, four different embedding rates, i.e., 0.1 *bpnc*, 0.2 *bpnc*, 0.3 *bpnc*, 0.4 *bpnc* are tested. In the training process, the effective features are selected according to the control parameter δ (δ is selected as 0.45, 0.46, 0.47, 0.48 or 0.49 in our testing) and a series of classifiers can be obtained. Then these obtained classifiers are used for testing.

As shown in Table 4, the proposed feature selection method can not only reduce the dimensionality of the merged feature vector, but also maintain a high detection accuracy rate. For example, when $\delta = 0.49$ and the embedding rate is 0.4 *bpnc*, for the merged feature set “SRM + JRM”, the dimension can be reduced from 57181 to 13482. Though the testing error is increased from 0.1667 to 0.1717, the detection accuracy rate is still better than using SRM (the testing error is 0.1988) and JRM (the testing error is 0. 2585) separately. When $\delta = 0.49$ and the embedding rate is 0.4 *bpnc*, for the merged feature set“SRM + JRM + DCTR”, the dimension can be reduced from 65181 to 16518. Though the testing error is increased from 0.1320 to 0.1340, the detection accuracy rate is still better than SRM (the testing error is 0.1988), JRM (the testing error is 0. 2585) or DCTR (the testing error is 0. 1504) separately.

Table 4. Features dimension and testing error of effective features

Embedding rates (*bpnc*)			Testing error			
			SRM + JRM	SRM + DCTR	JRM + DCTR	SRM + JRM + DCTR
0.1	$\delta = 0.49$	Dimension	13482	10406	9148	16518
		Testing error	0.4510	0.4393	0.4357	0.4356
	$\delta = 0.48$	Dimension	11557	8661	8382	14300
		Testing error	0.4510	0.4417	0.4358	0.4358
	$\delta = 0.47$	Dimension	9890	7122	7604	12308
		Testing error	0.4513	0.4418	0.4428	0.4367
	$\delta = 0.46$	Dimension	8348	5780	6940	10534
		Testing error	0.4515	0.4465	0.4446	0.4407
	$\delta = 0.45$	Dimension	7092	4742	6392	9113
		Testing error	0.4527	0.4467	0.4509	0.4419
0.2	$\delta = 0.49$	Dimension	13482	10406	9148	16518
		Testing error	0.3562	0.3287	0.3358	0.3278
	$\delta = 0.48$	Dimension	11557	8661	8382	14300
		Testing error	0.3588	0.3368	0.3369	0.3307
	$\delta = 0.47$	Dimension	9890	7122	7604	12308
		Testing error	0.3611	0.3418	0.3500	0.3421
	$\delta = 0.46$	Dimension	8348	5780	6940	10534
		Testing error	0.3646	0.3534	0.3570	0.3461
	$\delta = 0.45$	Dimension	7092	4742	6392	9113
		Testing error	0.3670	0.3599	0.3711	0.3492
0.3	$\delta = 0.49$	Dimension	13482	10406	9148	16518
		Testing error	0.2566	0.2279	0.2285	0.2189
	$\delta = 0.48$	Dimension	11557	8661	8382	14300
		Testing error	0.2592	0.2360	0.2317	0.2225
	$\delta = 0.47$	Dimension	9890	7122	7604	12308
		Testing error	0.2604	0.2407	0.2455	0.2310
	$\delta = 0.46$	Dimension	8348	5780	6940	10534
		Testing error	0.2683	0.2514	0.2527	0.2389
	$\delta = 0.45$	Dimension	7092	4742	6392	9113
		Testing error	0.2754	0.2609	0.2745	0.2442
0.4	$\delta = 0.49$	Dimension	13482	10406	9148	16518
		Testing error	0.1717	0.1398	0.1432	0.1340
	$\delta = 0.48$	Dimension	11557	8661	8382	14300
		Testing error	0.1722	0.1463	0.1459	0.1385
	$\delta = 0.47$	Dimension	9890	7122	7604	12308
		Testing error	0.1746	0.1524	0.1579	0.1452
	$\delta = 0.46$	Dimension	8348	5780	6940	10534
		Testing error	0.1820	0.1596	0.1686	0.1534
	$\delta = 0.45$	Dimension	7092	4742	6392	9113
		Testing error	0.1912	0.1733	0.1862	0.1565

4 Conclusions

In this paper, we propose a new universal JPEG steganalyzer. The contributions of this paper are as follows.

(1) A new feature merging method is proposed in this paper. Via merging features extracted from different domains, the detection accuracy rate of those existing JPEG steganalytic algorithms can be improved by 3% points or even higher.
(2) Considering about that the feature dimension is so high, a new feature selection method is also proposed in this paper. Experimental results demonstrate that it can not only achieve reduction of the dimensionality, but also maintain a high detection accuracy rate.

Acknowledgements. This work is partially supported by National Natural Science Foundation of China (61772572), Natural Science Foundation of Guangdong Province of China (2017A030313366), and the Fundamental Research Funds for the Central Universities (17lgjc45).

References

1. Cheddad, A., Condell, J., Curran, K., Kevitt, P.M.: Digital image steganography: survey and analysis of current methods. Sig. Process. **90**(3), 727–752 (2010)
2. Solanki, K., Sarkar, A., Manjunath, B.S.: YASS: yet another steganographic scheme that resists blind steganalysis. In: Furon, T., Cayre, F., Doërr, G., Bas, P. (eds.) IH 2007. LNCS, vol. 4567, pp. 16–31. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77370-2_2
3. Sarkar, A., Solanki, K., Manjunath, B.S.: Further study on YASS: steganography based on randomized embedding to resist blind steganalysis. In: Proceedings of the SPIE Security, Steganography, and Watermarking of Multimedia Contents X, San Jose, pp. 16–31. SPIE (2008)
4. Huang, F., Huang, J., Shi, Y.Q.: New channel selection rule for JPEG steganography. IEEE Trans. Inf. Forensics Secur. **7**(4), 1181–1191 (2012)
5. Huang, F., Luo, W., Huang, J., Shi, Y.Q.: Distortion function designing for JPEG steganography with uncompressed side-image. In: Proceedings of the First ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, 17–19 June 2013
6. Guo, L., Ni, J., Shi, Y.Q.: Uniform embedding for efficient JPEG steganography. IEEE Trans. Inf. Forensics Secur. **9**(5), 814–825 (2014)
7. Guo, L., Ni, J., Su, W., Tang, Ch., Shi, Y.Q.: Using statistical image model for JPEG steganography: uniform embedding revisited. IEEE Trans. Inf. Forensics Secur. **10**(12), 2669–2680 (2015)
8. Holub, V., Fridrich, J., Denemark, T.: Universal distortion function for steganography in an arbitrary domain. EURASIP J. Inf. Secur. **2014**, 1–13 (2014)
9. Li, B., Shi, Y.Q., Huang, J.: Steganalysis of YASS. In: Proceedings of the 10th ACM Multimedia & Security Workshop, Oxford, pp. 139–148. ACM (2008)
10. Fridrich, J., Goljan, M., Hogea, D.: Steganalysis of JPEG images: breaking the F5 algorithm. In: Petitcolas, F.A.P. (ed.) IH 2002. LNCS, vol. 2578, pp. 310–323. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36415-3_20

11. Kodovsky, J., Fridrich, J.: Quantitative steganalysis of LSB embedding in JPEG domain. In: Proceedings of the 12th ACM Workshop on Multimedia and Security, pp. 187–198. ACM (2010)
12. Liu, G., Huang, F., Li, Z.: Universal steganalysis against adaptive steganographic algorithms. J. Appl. Sci. **34**(5), 598–604 (2016). (in Chinese)
13. Goljan, M., Fridrich, J., Holotyak, T.: New blind steganalysis and its implications. In: Proceedings of the SPIE Security Steganography and Watermarking of Multimedia Contents VIII, vol. 6072, pp. 1–13 (2006)
14. Chen, C., Shi, Y.: JPEG image steganalysis utilizing both intrablock and interblock correlations. In: IEEE International Symposium on Circuits and Systems (ISCAS), pp. 3029–3032 (2008)
15. Fridrich, J.: Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In: Fridrich, J. (ed.) IH 2004. LNCS, vol. 3200, pp. 67–81. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30114-1_6
16. Pevny, T., Fridrich, J.: Merging Markov and DCT features for multiclass JPEG steganalysis. In: Proceedings of the SPIE, Electronic Imaging, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, pp. 301–314 (2007)
17. Kodovsky, J., Fridrich, J.: Calibration revisited. In: Proceedings of 11th ACM Multimedia & Security Workshop, pp. 7–8 (2009)
18. Kodovský, J., Fridrich, J., Holub, V.: Ensemble classifiers for steganalysis of digital media. IEEE Trans. Inf. Forensics Secur. **7**(2), 432–444 (2012)
19. Kodovsky, J., Fridrich, J.: Steganalysis of JPEG images using rich models. In: Proceedings of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XIV, San Francisco, CA, vol. 8303, 22–26 January 2012
20. Fridrich, J., Kodovsky, J.: Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensics Secur. **7**(3), 868–882 (2012)
21. Holub, V., Fridrich, J.: Low complexity features for JPEG steganalysis using undecimated DCT. IEEE Trans. Inf. Forensics Secur. **10**(2), 219–228 (2015)
22. Tan, Y., Huang, F., Huang, J.: Feature selection for high dimensional steganalysis. In: Shi, Y.-Q., Kim, H.J., Pérez-González, F., Echizen, I. (eds.) IWDW 2015. LNCS, vol. 9569, pp. 134–144. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-31960-5_12
23. Bas, P., Filler, T., Pevný, T.: "Break our steganographic system": the ins and outs of organizing BOSS. In: Filler, T., Pevný, T., Craver, S., Ker, A. (eds.) IH 2011. LNCS, vol. 6958, pp. 59–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24178-9_5