Detection for JPEG steganography based on evolutionary feature selection and classifier ensemble selection

Xiaofeng Ma[1, 2], Yi Zhang[1, 2], Xiaofeng Song[3], Chao Fan[2]
[1]State key Laboratory of Mathematical Engineering and Advanced Computing
Zhengzhou 450001, Henan, China
[2] Zhengzhou Science and Technology Institute, Zhengzhou 450001, Henan, China
[3] Xi'an Communication Institute, Xi'an 710106, Shanxi, China
[e-mail: fengye_xty@163.com, xiaofengsong@sina.com]
*Corresponding author: Xiaofeng Ma, Yi Zhang, Xiaofeng Song

Received May 4, 2017; revised July 11, 2017; accepted August 1, 2017; published November 30, 2017

Abstract

JPEG steganography detection is an active research topic in the field of information hiding due to the wide use of JPEG image in social network, image-sharing websites, and Internet communication, etc. In this paper, a new steganalysis method for content-adaptive JPEG steganography is proposed by integrating the evolutionary feature selection and classifier ensemble selection. First, the whole framework of the proposed steganalysis method is presented and then the characteristic of the proposed method is analyzed. Second, the feature selection method based on genetic algorithm is given and the implement process is described in detail. Third, the method of classifier ensemble selection is proposed based on Pareto evolutionary optimization. The experimental results indicate the proposed steganalysis method can achieve a competitive detection performance by compared with the state-of-the-art steganalysis methods when used for the detection of the latest content-adaptive JPEG steganography algorithms.

Keywords: JPEG steganography, steganalysis, detection, feature selection, classifier ensemble

This work was supported by the National Natural Science Foundation of China (No.61472447, 61379151 and 61602508).

https://doi.org/10.3837/tiis.2017.11.023 **ISSN : 1976-7277**

1. Introduction

Digital steganography is art of convert communication. It is often realized by embedding the secret messages into digital media such as image, audio, video and so on. As the ongoing communication behavior is covered by innocuous-looking digital media, the steganography can achieve good concealment and security. As the adversary of digital steganography, steganalysis [1] focuses on developing methods for detecting the presence of secret messages, estimating the message length, locating stego positions, extracting messages, etc. In recent years, with the ubiquitous availability of Internet services and multimedia applications, the steganography techniques are becoming more and more popular. Currently, there are thousands of steganography softwares with different platforms can be downloaded free of charge from the Internet. For the JPEG is one of the most popular image formats in social networks, image-sharing websites and Internet traffic, there exist numerous steganographic algorithms and the corresponding software tools for JPEG image. Therefore, the steganalysis of JPEG image is always a very active research topic in information hiding. Among all the steganalysis techniques for JPEG steganography, the detection technique for JPEG steganography is one of the most important techniques because the convert communication will fail only if the stego image is suspected [2].

As we know, the steganography techniques for digital image have made great progresses during the past 20 years, and the simple steganography methods such as LSB (Least Significant Bit) replacement, LSB matching have been substituted with highly undetectable content-adaptive steganography [3, 4, 5]. Currently, the content-adaptive JPEG steganography methods [6, 7, 8, 9, 10] are mostly designed based on an embedding distortion function and STCs (Syndrome-Trellis Codes) [11]. The steganography scheme defines an embedding distortion function related with the detectability firstly and then the messages are embedded by STCs which minimizes the distortion function at the same time. In contrast to non-adaptive steganography, the content-adaptive steganography constrains the embedding changes to edge, texture and noisy regions difficult to model and the embedding noise caused by content-adaptive steganography is covered by inherent image noise, so it can achieve the better statistical detectability and steganographic security.

With the content-adaptive scheme becomes the mainstream of JPEG steganography techniques, the corresponding steganalysis techniques also begin to attract more and more attentions. So far, many steganalysis methods have been proposed for the detection of content-adaptive JPEG steganography. Among these methods, most are designed based on the high dimensional statistical features [12, 13, 14, 15, 16, 17, 18, 19] and the ensemble classifier [20]. For example, in [12], CC-JRM (Cartesian Calibration JPEG Rich Model) feature was proposed based on a rich model of the DCT coefficients in a JPEG file, and CC-JRM can capture the embedding changes more comprehensive. In [13], the DCTR (Discrete Cosine Transform Residual) feature was proposed by convolving the decompressed JPEG image with 64 kernels of the DCT and extracting the first-order statistics of the quantized noise residuals. The DCTR feature can achieve better detection performance for content-adaptive JPEG steganography while preserving relatively low computational complexity. In [14], the PHARM (PHase-Aware pRojection Model) was proposed by utilizing the noise residuals of JPEG image and their phase with respect to an 8×8 grid. The PHARM feature can obtain better detection accuracy than DCTR. In [15] and [16], GFR (Gabor Filter Residual) feature was proposed based on two-dimensional (2D) Gabor filters which can describe image texture

effectively. The GRF feature improved the detection accuracy further for content-adaptive JPEG steganography often constrain the embedding changes to texture regions. In [17], GPDFR (Gauss Partial Derivative Filter Residual) feature was proposed and it can achieve the competitive detection performances with low computational complexity. In [18] and [19], the selection channel of content-adaptive JPEG steganography is considered for the extraction of steganalysis feature. The experimental results show that the steganalysis features that make use of the selection channel can improve the detection accuracy significantly, however, under this case, the steganography algorithm of stego image must be known. In addition, the steganalysis features proposed for the spatial image also can be used for the detection of JPEG steganography. For the dimensionality of the above features are all high, the final detections are performed by combining the high dimensional feature with an ensemble classifier [20].

According to the current research works for steganalysis of content-adaptive JPEG steganography, the designs of steganalysis feature and classifier are both important for the improvement of the detection accuracy. As to the design of the steganalysis feature, in order to capture the embedding changes more effectively, the proposed steganalysis features all include many feature subsets which are extracted for the detection of stego image from different aspects. Although the high dimensional feature can improve the detection accuracy to some extent, the time and space consumption will be increased. In particular, with the surging images in social network and Internet traffic, the efficiency of the steganalysis method is also becoming more and more important. In [21], a feature selection method for steganalysis was proposed based on genetic algorithm and ensemble classifier. The experimental results show the feature selection can improve the detection accuracy while reducing the feature dimensionality. However, this feature selection method is designed for individual feature component and the procedure is very time-consuming. In [22], the feature subsets are selected according to their detection performance. However, the selection strategy is greedy and local optimum, and the optimal feature set may not be found. As to the design of the classifier, in [20], for the high dimensional feature is difficult to train the widely popular Gaussian SVM (Support Vector Machine), the ensemble classifier was proposed and significantly lower training complexity. However, the optimum selection of the base classifiers do not be considered. In [23], a Bayesian ensemble classifier is used to give the final decisions for the suspicious image and the experimental results show the Bayesian strategy can improve the detection performance. In [24], the LCLSMR (Linear Classification using Least Squares Minimal Residual) classifier was proposed and it can offer certain potential advantages over the original ensemble leading to much lower computational complexity than the ensemble classifier. However, the detection is performed by only the individual classifier.

To improve the detection performance for content-adaptive JPEG steganography further, in this paper, a steganalysis method is proposed based on evolution feature selection and classifier ensemble selection. The proposed method integrates the steganalysis feature selection with the classifier ensemble selection into a whole to form a new steganalysis framework. First, the feature subsets are selected by genetic algorithm and the diverse feature sets can be obtained; then, the multiple linear classifiers are trained by the selected diverse feature sets respectively; last, the trained linear classifiers are selected by Pareto evolutionary optimization [25, 26] to form the final classifier set which decides the detection result by voting strategy. For the new steganalysis framework, the steganalysis feature selection and the classifier ensemble selection are combined to form the diverse feature set and the optimal classifier combination. Therefore, the detection accuracy would be improved while relatively few classifiers are used, which also means low computational complexity.

The rest of this paper is organized as follows. In Section 2, the framework of the proposed steganalysis method is given. In Section 3, the feature selection method is presented and the details are described. In Section 4, the classifier ensemble selection method is proposed and the corresponding algorithm is given. In Section 5, the experimental results are shown and discussed. In Section 6, the conclusions are drawn.

2. Framework of the proposed steganalysis method

The whole framework of the proposed steganalysis method is shown in **Fig. 1**. It can be seen that the new framework includes two stages: evolutionary feature selection and classifier ensemble selection. For the evolutionary feature selection, the construction of the high dimensional feature set $\mathbf{F}=(\mathbf{F}_1,\mathbf{F}_2,\ldots\mathbf{F}_n)$ is analyzed and then the feature set $\mathbf{F}$ is divided into different feature subsets $\mathbf{F}_1,\mathbf{F}_2,\cdots,\mathbf{F}_n$ firstly; second, the selector vector of feature subsets is coded into binary string and the feature selection is performed by genetic algorithm; last, the optimal feature sets $\mathbf{F}^1,\mathbf{F}^2,\cdots,\mathbf{F}^m$ can be obtained and all the selected feature sets are the subset of $\mathbf{F}$. For the classifier ensemble selection, first, the classifiers $C_1,C_2,\cdots,C_m$ are trained by the optimal feature sets $\mathbf{F}^1,\mathbf{F}^2,\cdots,\mathbf{F}^m$ respectively; second, the selector vector of classifiers is also coded into binary string and the classifiers are selected by Pareto evolutionary optimization [25, 26]; last, the optimal classifier set $C^1,C^2,\cdots,C^p(p<m)$ would be obtained. In the first stage, the encoding is executed for the solution and each gene represents a feature subset. In the second stage, the trained classifiers are selected by Pareto evolutionary algorithm, ttherefore, the encoding also need to be exected and each gene represents a classifier.

When steganalysis is performed for the suspicious JPEG image, the high dimensional feature $\mathbf{F}$ should be extracted firstly and then the detections are carried by the trained classifiers $C^1,C^2,\cdots,C^p$ respectively. The final detection result is decided by a classifier voting strategy.

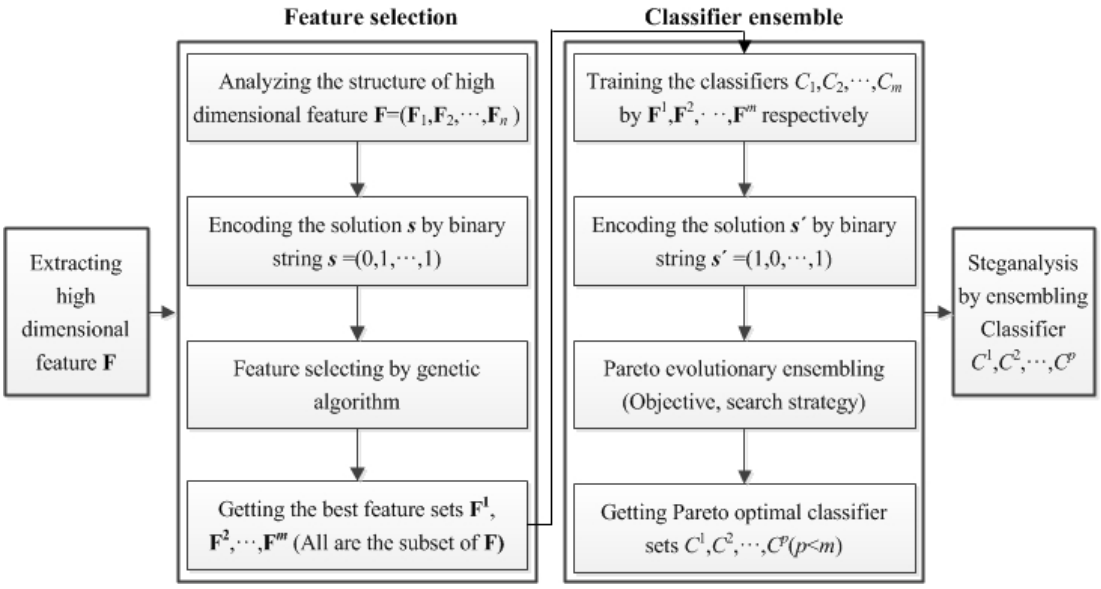

Fig. 1. Framework of the proposed steganalysis method based on evolutionary feature selection and classifier ensemble selection.

According to the above descriptions for the new steganalysis framework, it can be seen that the advantage of the proposed framework is the integration of the evolutionary feature selection and classifier ensemble selection. In the first stage, the optimal and diverse feature sets can be got by genetic algorithm which is effective for global optimization. In the second stage, the different classifiers are trained by the different feature sets which are outputs in the first stage, then, the classifier ensemble selection is performed by Pareto evolutionary optimization which considers the number of the classifiers and the detection accuracy at the same time. In summary, the integration of the feature selection and classifier ensemble selection can utilize the advantages of the high dimensional feature and ensemble strategy. In the following two sections, the feature selection based on genetic algorithm and the classifier ensemble selection based on Pareto evolutionary optimization are introduced respectively in detail.

3. Feature selection based on genetic algorithm

According to the process of high dimensional feature selection shown in **Fig. 1**, the whole feature set should be divided into nonoverlaping feature subsets firstly. For example, in [16], the GFR feature is extracted by 128 2D Gabor filters and the dimensionality of the feature set extracted by each filter is 170. Then, the GRF feature is constructed by merging and combing the different feature sets with 170 dimensions. For the corresponding feature sets of 2D Gabor filters with symmetry direction are merged, the GRF feature includes 72 feature subsets with 170 dimensions. In other words, GRF feature can be divided into 72 different nonoverlaping feature subsets. After the feature set is divided, to improve the detection accuracy and reduce computational complexity, the optimal feature subsets should be selected from all the feature subsets. In [27], the genetic algorithm [28] was used to optimize the performance of PM 1 (Plus Minus 1) steganography in JPEG images and the experimental results showed the capacity and security can be improved obviously. Here, the genetic algorithm is utilized for the selection of feature subsets which are used for the detection of content-adaptive JPEG steganography.

Let $\mathbf{F}=\{\mathbf{F}_1,\mathbf{F}_2,\ldots,\mathbf{F}_i,\ldots,\mathbf{F}_n\}$ denotes the high dimensional feature, $\mathbf{F}_i$ is the ith feature subset, $\boldsymbol{c}=\{0,1\}^n$ denotes a selector vector for all the feature subsets, $c_i=1$ means the ith feature subset is selected while $c_i=0$ means it is not selected. Further, $\mathbf{F}_{\boldsymbol{c}}$ denotes the corresponding feature set of the selector vector $\boldsymbol{c}$, $f(\mathbf{F}_{\boldsymbol{c}})$ denotes the evaluation value of the feature set $\mathbf{F}_{\boldsymbol{c}}$. Then, the selection of the feature $\mathbf{F}$ can be formulated as

$$\arg\min_{\boldsymbol{c}\in\{0,1\}^n} f(\mathbf{F}_{\boldsymbol{c}}). \tag{1}$$

In formula (1), $f(\mathbf{F}_{\mathbf{c}})$ is measured as the detection error rate of the steganalysis feature formed by $\mathbf{F}_{\mathbf{c}}$. Specially, it is measured by the total probability of error under equal Bayesian priors $P_E=(P_{FA}+P_{MD})/2$, with P_{FA} and P_{MD} the empirical probability of false alarm and missed detection respectively. The P_E is also always averaged over 10 splits on the image database and the proportion of training to testing sets is one-to-one.

According to the objective function shown in formula (1), the feature selection means to minimize the objective function $f(F_{\mathbf{c}})$ and the selector vector $\mathbf{c}$ is the solution. For genetic algorithm has achieve the good effects on different optimization problems, it is employed to search the optimal selector vector $\mathbf{c}$. When genetic algorithm is used for feature selection, the selector vector $\mathbf{c}$ is also the individual and the fitness function is denoted as $1/f(F_{\mathbf{c}})$. For $f(\mathbf{F}_{\mathbf{c}})=P_E$, the low detection error rate P_E of $\mathbf{F}_{\mathbf{c}}$ means the high fitness value of individual $\mathbf{c}$. The

calculation of the fitness value is shown in **Fig. 2**.

The procedure of the proposed selection method for steganalysis feature can be summarized in **Algorithm 1** and named as GSFS (Genetic Steganalysis Feature Selection). In addition, the crossover operator, mutation operator, population size, termination condition and so on also should be fixed and these details would be described in the experiments.

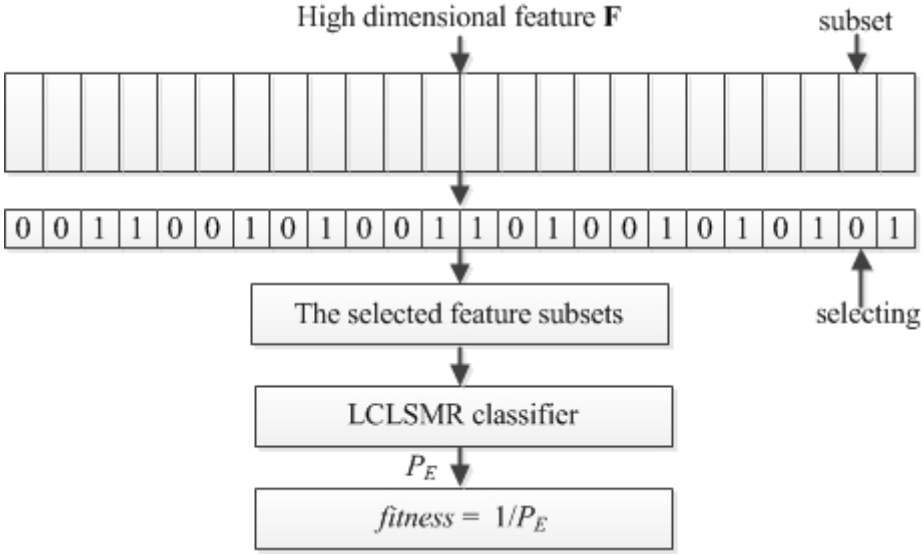

Fig. 2. Calculation of the fitness value of the solution for feature selection by genetic algorithm

Algorithm 1 The GSFS algorithm

Input:
Training feature set **F**;
Parameter settings of genetic algorithm.
Output: The selector vector ***c***.

1. Generate the set of the selector vector ***c*** randomly and the population *P* is formed by these selector vectors (individuals).
2. **Repeat**
3. Compute the fitness of each individual ***c*** in the population *P* according to the following formula,

$$fitness(\boldsymbol{c}) = 1/f(\mathbf{F}_c) \tag{2}$$

4. Perform the crossover operation for the population *P*;
5. Perform the mutation operation for the population *P*;
6. The next generation population *P* is generated by replace the parents with the better offspring;
7. Go to 3 until the stopping condition (generations and stall generation limit) is met.
8. **Output** the selector vector $\arg\min_{c\in P} f(\mathbf{F}_c)$

After the feature selection is performed by genetic algorithm, the optimal feature sets $\mathbf{F}^1,\mathbf{F}^2,\ldots,\mathrm{F}^m$ can be obtained and *m* is also the size of the final population. Then, the *m* feature sets are used to train the *m* classifiers respectively and a trained classifier set would be got.

4. Classifier ensemble selection based on Pareto optimization

By genetic algorithm, the optimal feature sets $\mathbf{F}^1,\mathbf{F}^2,\ldots,\mathrm{F}^m$ can be got and then the m classifiers are trained by different feature sets respectively. To improve the detection accuracy and reduce the computational complexity, some classifiers should be selected to form the final detector by ensemble strategy. For the number of classifiers and detection accuracy should be considered at the same time, the Pareto optimization algorithm is used for classifier ensemble selection.

Let $\boldsymbol{s}=\{0,1\}^m$ denotes the selector vector of classifiers, $s_i=1$ means the ith classifier is selected while $s_i=0$ means it is not be selected, C_s denotes the corresponding classifier set of the selector vector $\boldsymbol{s}$, $f(C_s)$ denotes the evaluation value of the selected classifier set C_s, which is measured by the detection accuracy P_E of C_s, $|\boldsymbol{s}|$ denotes the number of non-zero elements of the selector vector $\boldsymbol{s}$. Then, the ensemble selection of the classifiers can be formulated as the following bi-objective optimization problem.

$$\arg\min_{\boldsymbol{s}\in\{0,1\}^m}\left(f(C_s),|\boldsymbol{s}|\right). \tag{3}$$

For the bi-objective optimization problem shown in the above formula, the value of the objective function is a vector with two elements. In other words, the $f(C_s)$ and $|\boldsymbol{s}|$ will be considered at the same time. Therefore, the Pareto optimization is used to solve this problem, which is often used for multi-objective optimization problem. Here, the selector vector $\boldsymbol{s}$ is also the solution of the objective function, the calculation process of the bi-objective function value is shown in **Fig. 3**.

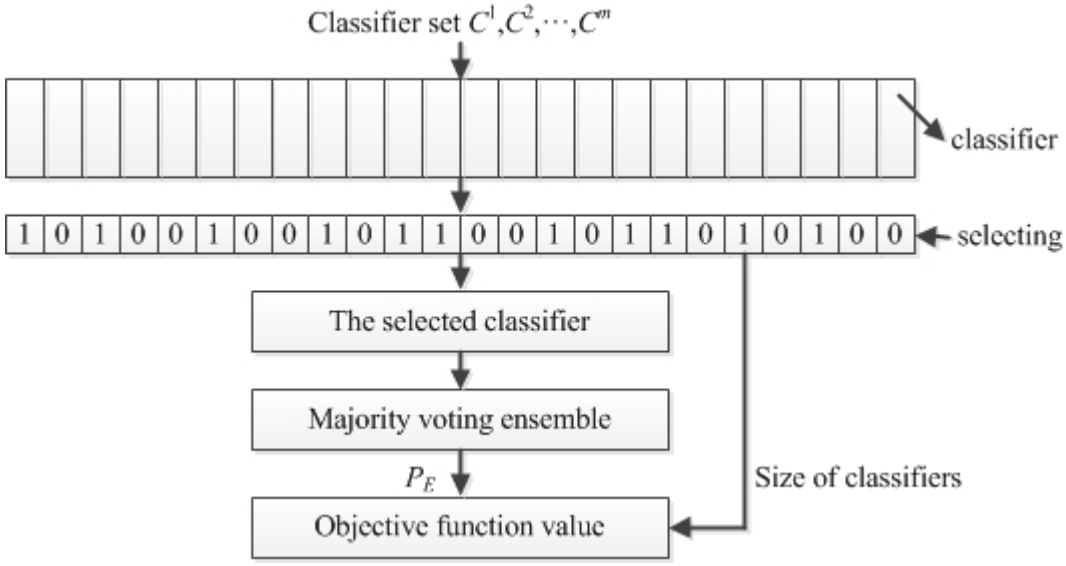

Fig. 3. Calculation of the objective function value for classifier ensemle selection by Pareto optimization

For the bi-objective optimization problem, the comparison between two solutions is not straightforward, because it is possible that one solution is better on the first objective while the other is better on the second objective. Therefore, the domination relationship is usually used for this special situation. Here, the domination relationship [25, 26] for bi-objective minimization problem can be defined as follows.

Let $g=(g_1,g_2)$ denotes the objective vector, S is the candidate solution set, two solutions $\boldsymbol{s},\boldsymbol{s}'\in S$, if $g_1(\boldsymbol{s})\le g_1(\boldsymbol{s}')$ and $g_2(\boldsymbol{s})\le g_2(\boldsymbol{s}')$, then $\boldsymbol{s}$ weakly dominates $\boldsymbol{s}'$, denoted as $\boldsymbol{s}\succeq\boldsymbol{s}'$; if $\boldsymbol{s}\succeq\boldsymbol{s}'$ and either $g_1(\boldsymbol{s})<g_1(\boldsymbol{s}')$ or $g_2(\boldsymbol{s})<g_2(\boldsymbol{s}')$, then $\boldsymbol{s}$ dominates $\boldsymbol{s}'$, denoted as $\boldsymbol{s}\succ\boldsymbol{s}'$.

For a solution $\boldsymbol{s}$, it is Pareto optimal if there is no other solution in S that dominates it. Accordingly, the bi-objective optimization problem may not have a single optimal solution, but instead have a set of Pareto optimal solutions. Last, one optimal solution is selected according to the preference, which is done through evaluation criterion function. For example, if the detection accuracy $f(C_s)$ is sensitive, the solution $\boldsymbol{s}$ with the best detection accuracy is selected, otherwise, if the number of the selected classifiers is sensitive, the solution $\boldsymbol{s}$ with small $|\boldsymbol{s}|$ is selected.

The minimization of the bi-objective function shown in formula (3) is based on a Pareto evolutionary optimization method. The detailed procedure can be summarized in **Algorithm 2** and named as PCES (Pareto Classifier Ensemble Selection).

Algorithm 2 The PCES algorithm

Input:
The trained classifier set $C_1,C_2,\ldots,C_m$;
The bi-objective function $(f(C_s), |\boldsymbol{s}|)$;
The evaluation criterion $eval(\cdot)$ of the solution.

Output: The selector vector $\boldsymbol{s}$.

1. Let $\boldsymbol{g}(\boldsymbol{s})=\left(\boldsymbol{f}(\boldsymbol{C}_s),|\boldsymbol{s}|\right)$ be the bi-objective function.

2. A solution $\boldsymbol{s}$ is generated randomly from $\{0,1\}^m$ and the candidate solution set $S=\{\boldsymbol{s}\}$;

3. Repeat

4. Select a solution $\boldsymbol{s}\in S$ and the new solution $\boldsymbol{s}'$ is generated by flipping the each bit with probability $1/n$.

5. If $\nexists\boldsymbol{z}\in P$ such that $\boldsymbol{z}\succ_{\boldsymbol{g}}\boldsymbol{s}'$, $S=\left(S-\left\{\boldsymbol{z}\in S\mid\boldsymbol{s}'\succeq_g\boldsymbol{z}\right\}\right)\cup\boldsymbol{s}'$.

6. The variable-deep search [29] is performed for the solution $\boldsymbol{s}'$ according to the following steps:

1) Let $Q=\{\},L=\{\}$, $\boldsymbol{N}(\cdot)$ denote the set of neighbor solutions with Hamming distance 1;

2) While $V_{s'}=\left\{\boldsymbol{y}\in\boldsymbol{N}(\boldsymbol{s}')\mid y_i\ne s_i',i\notin L\right\}\ne\varnothing$

Choose $\boldsymbol{y}\in V_{s'}$ with the minimal value f;

$Q=Q\cup\left\{\boldsymbol{y}\right\}$, $L=L\cup\left\{i\mid y_i\ne s_i'\right\}$, $\boldsymbol{s}'=\boldsymbol{y}$

3) Output the set Q.

7. for $\boldsymbol{q}\in Q$,

If $\nexists\boldsymbol{z}\in P$ such that $\boldsymbol{z}\succ_{\boldsymbol{g}}\boldsymbol{q}$, $S=\left(S-\left\{\boldsymbol{z}\in S\mid\boldsymbol{q}\succeq_g\boldsymbol{z}\right\}\right)\cup\boldsymbol{q}$

8. **Output** the solution $\arg\min_{s\in S}eval(\boldsymbol{s})$ according to the preference.

In this paper, the evaluation criterion $eval(\cdot)$ of solution $\boldsymbol{s}$ is the detection accuracy P_E of the corresponding selected classifier set C_s. If the size of the selected classifier set is sensitive, the solution can be selected according to the number of classifiers.

5. Experimental Results and Analysis

In this section, the image database and experimental setup are introduced firstly. Then, the proposed feature selection method is evaluated by the GFR feature which has the best detection performance for the J-UNIWARD (JPEG Universal Wavelet Relative Distortion) [7] steganography. Third, the proposed ensemble selection method for classifier is validated based on the feature selection. Last, according to the detection performances for the three content-adaptive JPEG steganography algorithms such as UED (Uniform Embedding Distortion) [8], J-UNIWARD [7] and SI-UNIWARD (Side-Informed UNIWARD) [7], the proposed steganalysis method is compared with the other state-of-the-art steganalysis methods.

5.1 Image database and experiment setup

In the experiments, BOSSbase 1.01 database is used. This database contains 10,000 grayscale 512 × 512 images in PGM format. For the UED and J-UNIWARD steganography, all images were converted into JPEG images with QFs 75 and 95, and the corresponding stego images were generated with 0.05, 0.1, 0.15, 0.2, 0.3, 0.4 and 0.5 bpac (bit per non-zero AC DCT coefficient) payloads. For the SI-UNIWARD steganography, the original grayscale images were used as precover images, and then the corresponding stego images were generated with payloads from ranging from 0.05 bpac to 0.5 bpac when the grayscale images are compressed to JPEG images with quality factors 75 and 95. Hence, for each steganography algorithm and QF (quality factor), we have one group of cover images and seven groups of stego images. One group of cover images and one of group corresponding stego images are used as the image samples for one payload.

In all experiments, the proportion of training to testing set was one-to-one and the P_E was used to evaluate the detection performance of the different steganalysis methods. The detection accuracy P_E is the average over 10 random 5000/5000 splits on the image set.

5.2 Effect of the feature selection by genetic algorithm

In this subsection, the effect of the proposed feature selection method is evaluated according to the detection performance for J-UNIWARD steganography by GFR feature. The GFR features were selected for the design because they are known to be highly effective against modern JPEG steganography [30]. The 2D Gabor filters can describe image texture features from different scales and orientations. Thus, the GFR can achieve the state-of-the-art performance in most of the cases when steganalyzing adaptive JPEG steganography.In this experiment, the quality factor of JPEG image is 75, the payload of stego image is 0.3bpac, the dimensionality of the GFR feature is 12240 and it includes 72 feature subsets with 170 dimensions.

According to the characteristic of GFR feature, the individual $\boldsymbol{s}$ of the genetic algorithm should be a binary string with 72 elements. In addition, the size of the population is 100, the selection strategy is tournament and tournament size is 2, the crossover operator is scattered crossover, the mutation operator is uniform mutation and the probability is 0.1, the elite count is 2, the number of the iterations is 60, the stall generations is 10, the function *ga* in Matlab R2016b is used for the feature selection.

Fig. 4 shows the detection accuracy of each feature subset of GFR feature. According to **Fig. 4**, it can be seen that the detection accuracies of the 72 feature subsets of GFR are various. When the feature selection is performed by genetic algorithm, the feature subset with the high detect accuracy should be selected as one part of the final steganalysis feature with high probability.

Fig. 5 show the best P_E and mean P_E of the individuals during the iterative process of evolutionary feature selection by genetic algorithm. It can be seen that the best P_E and mean P_E are both gradually improved. This certifies the proposed feature selection method is effective. In addition, it should be noticed that the improvement becomes smaller and smaller with the iterative progress of the genetic algorithm.

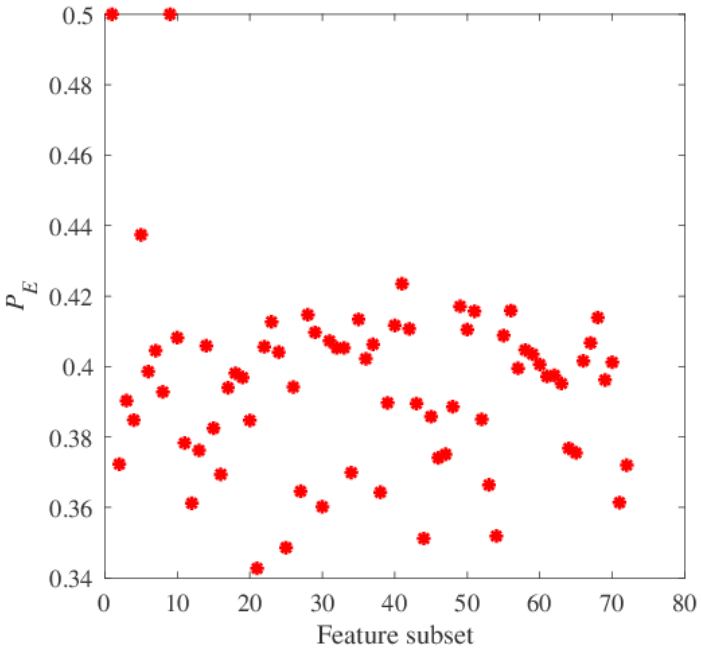

Fig. 4. Detection error P_E of the 72 different feature subsets included in GFR feature for J-UNIWARD with quality factors 75 and payload 0.3bpac.

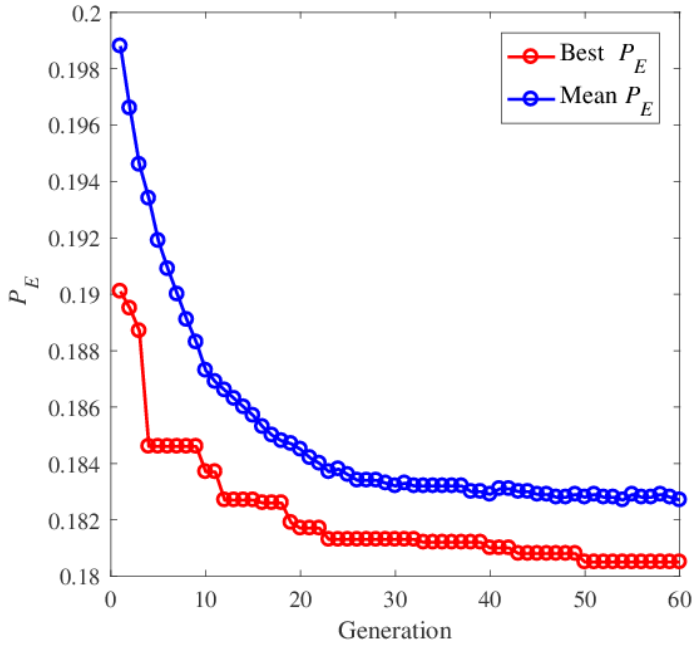

Fig. 5. The best and mean detection error P_E of the individuals during the iterative process of feature selection by genetic algorithm for GFR for J-UNIWARD with quality factors 75 and payload 0.3bpac.

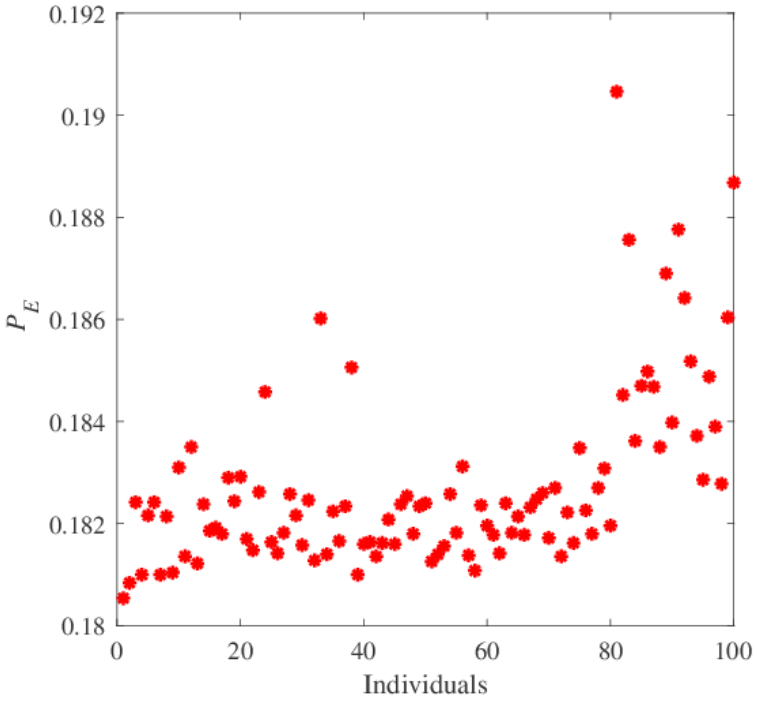

Fig. 6. Detection error P_E of the corresponding feature of each individual in the final population for J-UNIWARD with quality factors 75 and payload 0.3bpac.

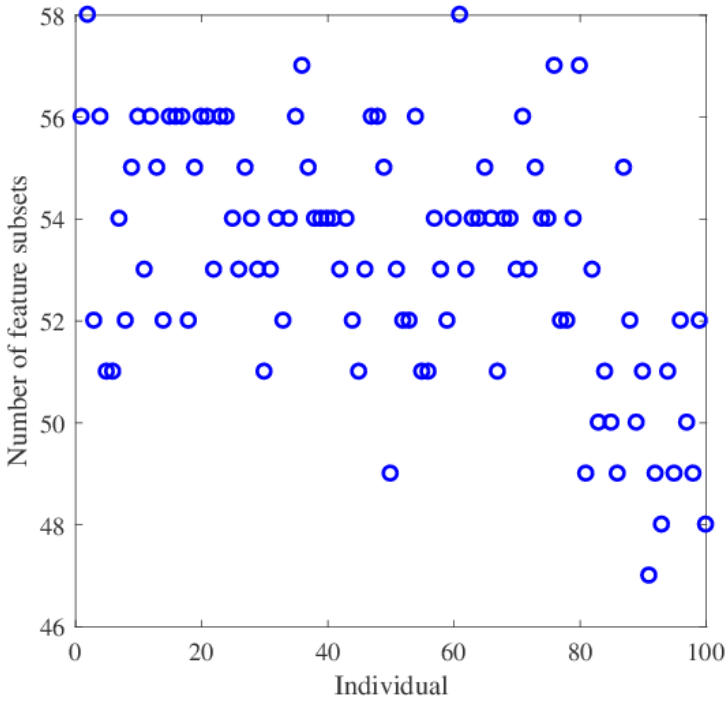

Fig. 7. Number of the feature subsets included in each individual in the final population when feature selection is performed for GFR for J-UNIWARD with quality factors 75 and payload 0.3bpac.

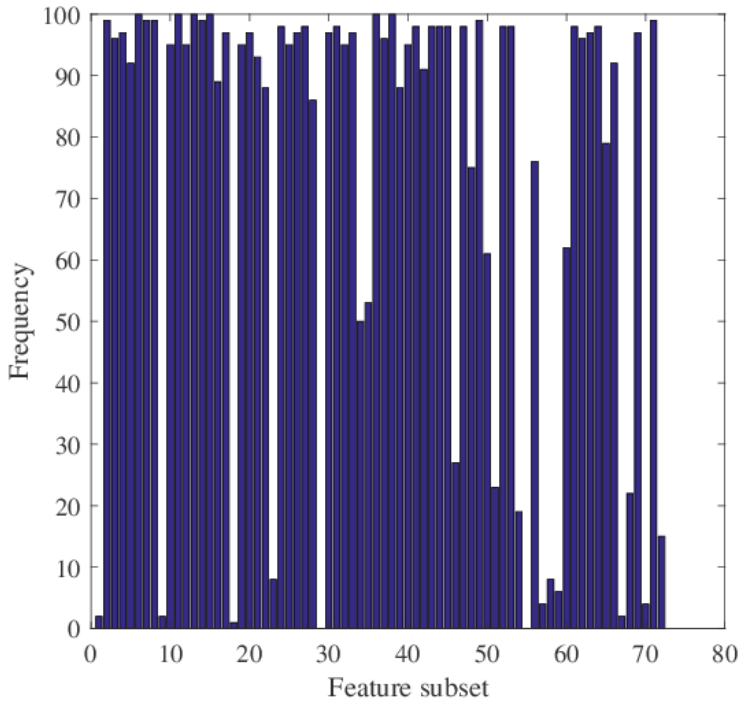

Fig. 8. Occurrence frequency of the feature subsets over all the individuals of the final population when feature selection is performed for GFR for J-UNIWARD with quality factors 75 and payload 0.3bpac.

After 60 iterations, the final population which includes 100 individuals is obtained. **Fig. 6** shows the detection error P_E of the corresponding steganalysis feature of each individual. **Fig. 7** shows the number of the feature subsets included in each individual. **Fig. 8** shows the occurrence frequency of each feature subset. As shown in **Fig. 6**, the detection accuracy of the corresponding steganalysis feature of each individual is also different, this is because the different steganalysis feature includes different feature subsets. According to **Fig. 7**, it can be seen that the number of the feature subsets included in each individual is variable, the maximum number is 58 and the minimum number is 47. According to **Fig. 4** and **Fig. 8**, it can be seen that the occurrence frequency of each feature subset is different and the better detection accuracy means the high occurrence frequency.

In summary, the diverse and effective feature sets can be got after the feature selection by genetic algorithm has been performed. Then, these different feature sets would be used to train the different classifiers and form the trained classifier set.

5.3 Effect of classifier ensemble selection by Pareto optimization

According to the proposed steganalysis framework shown in **Fig. 1**, the classifiers should be trained by the optimal feature sets generated by genetic algorithm firstly, and then the trained classifiers are selected to form the final ensemble classifier based on Pareto evolutionary optimization. In this subsection, the detection performances of the four different steganalysis methods are compared. In the experiment, the JPEG steganography algorithm is J-UNIWARD, the steganalysis feature is GFR, the dimensionality of the GFR feature is 12240 and it includes 72 feature subsets with 170 dimensions, the quality factor of JPEG image is 75, the payload of stego image is 0.3bpac. The feature selection is perform according to **Algorithm 1** and the parameter settings of genetic algorithm are same to the above subsection. Last, the 100

different optimal feature sets are obtained.

The four different steganalysis methods are based on the different classifiers. The first steganalysis method is based on ensemble classifier (EC) and the second steganalysis method is based on LCLSMR. For these two steganalysis methods, the steganalysis feature is extracted firstly and then the EC or LCLSMR is used for training and testing. The third steganalysis method is named as FSBEL (Feature Selection Based Ensemble LCLSMR). For this method, after feature extraction, the feature selection needs to be performed according to **Algorithm 1**, then the different LCLSMR classifiers are trained by the several best feature sets, last, the final detection result is determined by voting strategy. The fourth steganalysis method is the proposed method in this paper, the difference between the proposed method and the FSBL is the construction of the final detector. The former selects the trained classifiers by Pareto evolutionary optimization and the selected classifiers are used to form the final detector.

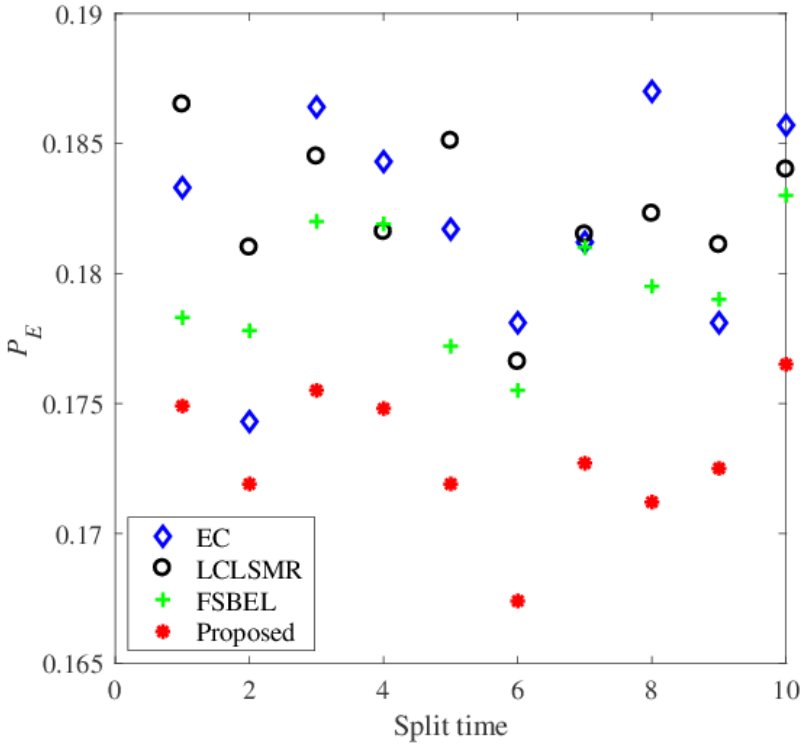

Fig. 9. Detection error P_E of the four steganalysis methods over ten image database splits when detection is performed for J-UNIWARD with quality factors 75 and payload 0.3bpac.

Fig. 9 shows the detection accuracies P_E of the four different steganalysis methods over ten image database splits into 5000/5000 training/testing images. For each image database splits, the corresponding training and testing set are constructed, and then the relevant classifiers are trained and the testing is performed. As the training and testing set are different for each image database splits, the detection accuracies are also changing. According to the experimental results shown in **Fig. 9**, it can be seen that the proposed steganalysis method can achieve the best detect performances. The FSBEL method can achieve the better detection performances than EC and LCLSMR. This is because that the diverse and optimal feature sets can be got by feature selection based on genetic algorithm and the ensemble of the classifiers trained by the optimal feature sets improves the detection accuracy. In contrast to FSBEL, the proposed

steganaysis method selects the classifiers by Pareto evolutionary algorithm and this can get the better detection performance with relatively few classifiers. In the ten image database splits, the number of the selected classifiers from the 100 classifiers is at most 21 and at least 7.

5.4 Comparison to prior art

In this subsection, the four different steganalysis methods are compared for the detection performance of UED, J-UNIWARD and SI-UNIWARD. The steganalysis features are DCTR, PHARM and GFR respectively. The parameter settings of genetic algorithm is same to subsection 5.2 and 5.3.

Table 1. Detection error P_E of the different steganalysis methods with DCTR feature

Steg	Payload	QF=75				QF=95			
		EC	LCLSMR	FSBEL	FSBPEL	EC	LCLSMR	FSBEL	FSBPEL
UED	0.05	0.4248	0.4283	0.4175	**0.4153**	0.4845	0.4893	0.4821	**0.4801**
	0.10	0.3611	0.3672	0.3543	**0.3501**	0.4596	0.4623	0.4552	**0.4513**
	0.20	0.2118	0.2194	0.2045	**0.1987**	0.3937	0.3974	0.3910	**0.3887**
	0.30	0.1121	0.1164	0.1035	**0.1003**	0.3145	0.3182	0.3103	**0.3065**
	0.40	0.0611	0.0634	0.0581	**0.0547**	0.2199	0.2231	0.2146	**0.2111**
	0.50	0.0213	0.0247	0.0189	**0.0167**	0.1251	0.1312	0.1203	**0.1185**
J-UNI WARD	0.05	0.4776	0.4803	0.4745	**0.4723**	0.4989	0.4999	0.4978	**0.4953**
	0.10	0.4359	0.4396	0.4312	**0.4273**	0.4850	0.4886	0.4822	**0.4803**
	0.20	0.3379	0.3412	0.3341	**0.3289**	0.4541	0.4573	0.4500	**0.4489**
	0.30	0.2409	0.2451	0.2342	**0.2301**	0.3999	0.4079	0.3958	**0.3934**
	0.40	0.1555	0.1597	0.1489	**0.1423**	0.3358	0.3396	0.3311	**0.3276**
	0.50	0.0920	0.0978	0.0867	**0.0845**	0.2587	0.2643	0.2523	**0.2489**
SI-UNI WARD	0.05	0.4990	0.4998	0.4967	**0.4934**	0.4722	0.4785	0.4678	**0.4653**
	0.10	0.4977	0.4985	0.4942	**0.4917**	0.4746	0.4789	0.4712	**0.4697**
	0.20	0.4829	0.4857	0.4774	**0.4753**	0.4645	0.4674	0.4611	**0.4592**
	0.30	0.4586	0.4612	0.4556	**0.4513**	0.4585	0.4613	0.4553	**0.4521**
	0.40	0.4070	0.4123	0.4042	**0.4011**	0.4272	0.4310	0.4233	**0.4201**
	0.50	0.3410	0.3479	0.3353	**0.3321**	0.3757	0.3810	0.3722	**0.3695**

Table 2. Detection error P_E of the different steganalysis methods with PHARM feature

Steg	Payload	QF=75				QF=95			
		EC	LCLSMR	FSBEL	FSBPEL	EC	LCLSMR	FSBEL	FSBPEL
UED	0.05	0.4125	0.4177	0.4085	**0.4063**	0.4805	0.4857	0.4765	**0.4743**
	0.10	0.3285	0.3321	0.3247	**0.3189**	0.4472	0.4508	0.4413	**0.4386**
	0.20	0.1732	0.1786	0.1700	**0.1612**	0.3747	0.3795	0.3701	**0.3666**
	0.30	0.0831	0.0885	0.0783	**0.0733**	0.2833	0.2889	0.2795	**0.2754**
	0.40	0.0411	0.0452	0.0486	**0.0365**	0.1955	0.2011	0.1913	**0.1844**
	0.50	0.0155	0.0135	0.0135	**0.0110**	0.1132	0.1176	0.1089	**0.1043**
J-UNI WAR D	0.05	0.4677	0.4723	0.4635	**0.4602**	0.4957	0.4986	0.4935	**0.4917**
	0.10	0.4285	0.4323	0.4234	**0.4203**	0.4816	0.4874	0.4782	**0.4759**
	0.20	0.3114	0.3167	0.3085	**0.3022**	0.4360	0.4425	0.4312	**0.4283**
	0.30	0.2042	0.2087	0.2005	**0.1934**	0.3745	0.3796	0.3711	**0.3640**
	0.40	0.1227	0.1278	0.1186	**0.1134**	0.3105	0.3168	0.3044	**0.3001**
	0.50	0.0753	0.0811	0.0711	**0.0687**	0.2257	0.2300	0.2192	**0.2133**
SI-U NIW ARD	0.05	0.4950	0.4989	0.4923	**0.4901**	0.4877	0.4900	0.4853	**0.4831**
	0.10	0.4956	0.4987	0.4911	**0.4887**	0.4870	0.4898	0.4847	**0.4822**
	0.20	0.4785	0.4812	0.4745	**0.4713**	0.4854	0.4875	0.4832	**0.4810**
	0.30	0.4525	0.4583	0.4498	**0.4475**	0.4745	0.4780	0.4711	**0.4689**
	0.40	0.3989	0.4022	0.3954	**0.3921**	0.4476	0.4513	0.4430	**0.4412**
	0.50	0.3353	0.3396	0.3302	**0.3241**	0.4029	0.4067	0.4002	**0.3977**

Table 3. Detection error P_E of the different steganalysis methods with GFR feature

Steg	Payload	QF=75				QF=95			
		EC	LCLSMR	FSBEL	FSBPEL	EC	LCLSMR	FSBEL	FSBPEL
UED	0.05	0.4094	0.4123	0.4057	**0.4015**	0.4781	0.4823	0.4745	**0.4712**
	0.10	0.3170	0.3215	0.3147	**0.3086**	0.4457	0.4497	0.4400	**0.4376**
	0.20	0.1671	0.1724	0.1633	**0.1592**	0.3621	0.3693	0.3574	**0.3501**
	0.30	0.0828	0.0853	0.0797	**0.0774**	0.2751	0.2811	0.2703	**0.2601**
	0.40	0.0350	0.0366	0.0331	**0.0318**	0.1700	0.1769	0.1645	**0.1582**
	0.50	0.0144	0.0179	0.0132	**0.0127**	0.1048	0.1112	0.1001	**0.0975**
J-UNI WARD	0.05	0.4629	0.4675	0.4594	**0.4571**	0.4938	0.4976	0.4910	**0.4895**
	0.10	0.4158	0.4190	0.4111	**0.3987**	0.4801	0.4862	0.4765	**0.4721**
	0.20	0.2974	0.3014	0.2925	**0.2883**	0.4297	0.4365	0.4243	**0.4200**
	0.30	0.1847	0.1889	0.1800	**0.1729**	0.3655	0.3714	0.3604	**0.3572**
	0.40	0.1054	0.1102	0.1013	**0.0968**	0.2893	0.2941	0.2854	**0.2781**
	0.50	0.0516	0.0568	0.0475	**0.0443**	0.2124	0.2173	0.2071	**0.2011**
SI-UNI WARD	0.05	0.4958	0.4995	0.4924	**0.4913**	0.4866	0.4927	0.4822	**0.4804**
	0.10	0.4936	0.4972	0.4914	**0.4895**	0.4810	0.4879	0.4777	**0.4765**
	0.20	0.4751	0.4786	0.4721	**0.4700**	0.4736	0.4795	0.4700	**0.4682**
	0.30	0.4421	0.4475	0.4389	**0.4364**	0.4605	0.4672	0.4563	**0.4512**
	0.40	0.3916	0.3974	0.3885	**0.3832**	0.4223	0.4287	0.4195	**0.4141**
	0.50	0.3320	0.3371	0.3259	**0.3210**	0.3762	0.3826	0.3710	**0.3645**

In **Table 1**, the detection accuracies of the four different steganalysis methods with DCTR feature are presented for the three content-adaptive JPEG steganography schemes with quality factors 75 and 95. The experimental results show the proposed FSBPEL (Feature Selection Based Pareto Ensemble LCLSMR) can achieve the best detection performances. The genetic algorithm based feature selection contributes to the formation of the optimal feature set and the Pareto optimization based classifier selection can get the better ensemble results. That is to say, the proposed steganalysis method integrates the advantages of the feature selection and classifier selection.

In **Table 2** and **Table 3**, the detection accuracies of the four different steganalysis methods with PHARM and GFR feature are presented respectively. The experimental results also show the proposed FSBPEL method can achieve the best detection performances.

The time consumption of the four different steganalysis methods is shown in **Table 4** and the detection time consumption is given in bold. All steganalysis methods were implemented in Matlab 2015a and run on an Intel i7 4.0 GHz. According to **Table 4**, it can be seen that the FSBPEL are relatively more time-consuming than other steganalysis methods. This is because the feature selection, classifier selection and detection are all need to be executed and the time consumption of the three stages are 4166.7, 315.9 and 388.2 respectively. Obviously, the feature selection by genetic algorithm is relatively time-consuming, however, the feature selection only needs to be executed once for classifier training. The detection time consumption of FSBPEL is only longer than LCLSMR which is the cost for the improvement in detection accuracy.

Table 4. Time consumption of the four different steganalysis methods (in seconds)

Steganalysis method	EC	LCLSMR	FSBEL	FSBPEL
Time consumption	**573.8**	**55.5**	4166.7+**514.9**	4166.7+315.9+**388.2**

6. Conclusion

In this paper, a new steganalysis method for content-adaptive JPEG steganography is proposed by integrating the evolutionary feature selection and classifier ensemble selection. The proposed steganalysis method includes two parts: the former performs the feature selection based on genetic algorithm and this can form the optimal feature sets used to train the different

classifiers respectively; the latter performs the classifier ensemble selection based on Pareto evolutionary optimization and it can improve the detection accuracy while reduce the number of the selected classifiers. The integration of feature selection and classifier ensemble selection can take the advantages of the rich steganalysis feature and ensemble strategy. Recently, the steganalysis method based on deep learning are becoming more and more attractive and some excellent works have been done [31, 32, 33, 34, 35]. In the future, we will explore the integration of the proposed steganalysis method with the deep learning. For example, the detection performance of deep CNN (convolution neural network) may be improved by Pareto evolutionary ensemble selection of CNN with different parameter settings.

References

[1] J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications, Cambridge University Press, Cambridge, 2010.

[2] H. Q. Wang, S. Z. Wang, "Cyber warfare: steganography vs. steganalysis," *Communications of the ACM*, vol. 47, no. 10, pp. 76-82, October, 2004. Article (CrossRef Link)

[3] T. Pevný, T. Filler, P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc of the 12th International Workshop on Information Hiding*, pp. 161-177, June 28-30, 2010. Article (CrossRef Link)

[4] B. Li, M. Wang, X. L. Li, S. Q. Tan, J. W. Huang, "A strategy of clustering modification directions in spatial image steganography," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1905-1917, September, 2015. Article (CrossRef Link)

[5] W. M. Zhang, Z. Zhang, L. L. Zhang, H. Y. Li N. H. Yu, "Decomposing Joint Distortion for Adaptive Steganography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol.PP, no.99, pp.1-1, July, 2016. Article (CrossRef Link)

[6] F. J. Huang, J. W. Huang, Y. Q. Shi, "New Channel Selection Rule for JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1181-1191, August, 2012. Article (CrossRefLink)

[7] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," *in Proc. of 1st ACM IH&MMSec. Workshop*, pp.59-68, June 20-22, 2013. Article (CrossRef Link)

[8] L. J. Guo, J. Q. Ni, Y. Q. Shi, "Uniform embedding for efficient JPEG steganography," *IEEE Transactions on Information Forensics and Security*, vol.9, no.5, pp. 814-825, May, 2014. Article (CrossRef Link)

[9] F. Y. Li, X. P. Zhang, J. Yu, W. F, Shen, "Adaptive JPEG steganography with new distortion function," *Annals of Telecommunications*, vol. 69, no. 7, pp. 431-440, August, 2014. Article (CrossRef Link)

[10] Z. C. Wang, X. P. Zhang, Z. X. Yin, "Hybrid distortion function for JPEG steganography," *Journal of Electronic Imaging*, vol. 25, no. 5, pp. 050501, September, 2016. Article (CrossRef Link)

[11] 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, September, 2011. Article (CrossRef Link)

[12] 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*, pp. 0A 1-13, January 22-26, 2012. Article (CrossRefLink)

[13] V. Holub and J. Fridrich, "Low Complexity Features for JPEG Steganalysis Using Undecimated DCT," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 219–228, February, 2015. Article (CrossRefLink)

[14] V. Holub, J. Fridrich, "Phase-Aware Projection Model for Steganalysis of JPEG Images," *in Proc. of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XIV*, pp. 94090T-94090T-11, February 8-12, 2015. Article (CrossRefLink).

[15] X. F. Song, F. L. Liu, C. F. Yang, X. Y. Luo and Y. Zhang, "Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters," in *Proc. of the 3rd ACM Workshop on Information Hiding and Multimedia Security*, pp. 15-23, June 17-19, 2015. Article (CrossRefLink).
[16] X. F. Song, F. L. Liu, C. F. Yang, X. Y. Luo, "2D Gabor Filters based steganalysis of content-adaptive JPEG Steganography," *Multimedia Tools and Application*, December, 2016. Article (CrossRefLink)
[17] Y. Zhang, F. L. Liu, C. F. Yang, et al, "Steganalysis of content-adaptive JPEG steganography based on Gauss partial derivative filter bank," *Journal of Electronic Imaging*, vol. 26, no. 1, pp. 013011-013011, February, 2017. Article (CrossRefLink)
[18] X. F. Song, F. L. Liu, C. F. Yang, et al, "Steganalysis of Adaptive JPEG Steganography by Selecting DCT Coefficients According to Embedding Distortion," *KSII Transactions on Internet and Information Systems*, vol. 9, no. 12, pp. 5209-5228, December, 2015. Article (CrossRefLink)
[19] T. Denemark, M. Boroumand, J. Fridrich, "Steganalysis Features for Content-Adaptive JPEG Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1736–1746, August, 2016. Article (CrossRefLink)
[20] 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, April, 2012. Article (CrossRefLink)
[21] V. Sachnev, H. J. Kim, "Binary Coded Genetic Algorithm with Ensemble Classifier for feature selection in JPEG steganalysis," *in Proc of the 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp.1-6, April 21-24, 2014. Article (CrossRefLink)
[22] B. Cao, G. R. Feng, Z. X. Yin, "Optimizing Feature for JPEG Steganalysis via Gabor Filter and Co-occurrences Matricesm," in *Proc of the International Conference on Cloud Computing and Security*, pp.84-93, July 29-31, 2016. Article (CrossRefLink)
[23] F. Y. Li, X. P. Zhang, B. Chen, et al, "JPEG steganalysis with high-dimensional features and Bayesian ensemble classifier," *IEEE Signal Processing Letters*, vol.20, no. 3, pp.233-236, March, 2013. Article (CrossRefLink)
[24] R. Cogranne, V. Sedighi, J. Fridrich, et al, "Is ensemble classifier needed for steganalysis in high-dimensional feature spaces?," in *Proc of the IEEE International Workshop on Information Forensics and Security*, pp.1-6, November, 2015. Article (CrossRefLink)
[25] R. T. Marler, J. S. Arora, "Survey of multi-objective optimization methods for engineering," *Structural and multidisciplinary optimization*, vol. 26, no. 6, pp. 369-395, April, 2004. Article (CrossRefLink)
[26] C. L. Qian, Y. Yu, Z. H, Zhou. "Pareto Ensemble Pruning," in *Proc of the Twenty-Ninth AAAI Conference on Artificial Intelligence*, pp. 2935-2941, January, 2015. Article (CrossRefLink)
[27] L. F. Yu, Y. Zhao, R. R. Ni, Z. F. Zhu. "PM1 steganography in JPEG images using genetic algorithm," *Soft Computing*, vol. 13, no. 4, pp. 393-400, February, 2009. Article (CrossRefLink)
[28] D. Whitley, "A genetic algorithm tutorial," *Statistics and computing*, vol. 4, no. 2, pp. 65-85, June, 1994. Article (CrossRefLink)
[29] S. Lin, B. W. Kernighan, "An effective heuristic algorithm for the traveling-salesman problem," *Operations research*, vol.21, no.2, pp. 498-516, April, 1973. Article (CrossRefLink)
[30] T. Denemark, J. Fridrich, "Steganography with Multiple JPEG Images of the Same Scene," *IEEE Transactions on Information Forensics and Security*," vol.12, no.10, pp. 2308-2319, October, 2017. Article (CrossRefLink)
[31] S. Q. Tan, B. Li, "Stacked convolutional auto-encoders for steganalysis of digital images," *in Proc of Asia-Pacific Signal and Information Processing Association Annual Summit and Conference*, pp.1-4, December 9-12, 2015. Article (CrossRefLink)
[32] Y. L. Qian, J. Dong, W. Wang, et al, "Deep learning for steganalysis via convolutional neural networks," in *Proc of SPIE Media Watermarking, Security, and Forensics 2015, Part of IS&T International Symposium on Electronic Imaging*," pp. 94090J-94090J-10, 2015. Article (CrossRefLink)
[33] G. S. Xu, H. Z. Wu, Y. Q. Shi, "Structural Design of Convolutional Neural Networks for Steganalysis," *IEEE Signal Processing Letters*, vol.23, no.5, pp.708-712, May, 2016.

Article (CrossRefLink)
[34] J. S. Zeng, S. Q. Tan, B. Li, et al, "Large-scale JPEG steganalysis using hybrid deep-learning framework," arXiv preprint arXiv:1611.03233v2, 2017. Article (CrossRefLink)
[35] M. Chen, V. Sedighi, M. Boroumand, J. Fridrich, "JPEG-Phase-Aware Convolutional Neural Network for Steganalysis of JPEG Images," in *Proc. of the 5rd ACM Workshop on Information Hiding and Multimedia Security*, pp. 75-84, June 20-22, 2017. Article (CrossRefLink)

Xiaofeng Ma 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 Information security, digital image forensic, analysis and processing of social media.

Yi Zhang received his BE degree from Xidian University, Xi'an, China, in 2010, and his MS degree from Zhengzhou Science and Technology Institute, Zhengzhou, China, in 2013. He is currently working toward his PhD at Zhengzhou Science and Technology Institute. His research interest includes digital image steganography and steganalysis technique.

Xiaofeng Song received the B.S. degree from the School of Information and Technology, Zhengzhou University, Zhengzhou, China, in 2002, M.S. degree from the School of Computer Science, Xidian University, Xi'an, China, in 2009, and PhD from Zhengzhou Science and Technology Institute, Zhengzhou, China, in 2009, 2012, and 2016. Now, he is a lecturer with Xi'an Communication Institute, Xi'an, China. His current research interest includes steganography, steganalysis and digital image forensic.

Chao Fan received his BS and MS degrees and PhD from Zhengzhou Science and Technology Institute, Zhengzhou, China, in 2009, 2012, and 2016, respectively. Currently, he is a lecturer with Zhengzhou Science and Technology Institute. His current research interests include digital image processing and forensics.