PFA-based feature selection for image steganalysis

Madhavi B. Desai*

CE/IT Department,
CGPIT, Uka Tarsadia University,
Maliba Campus, Gopal Vidyanagar,
Bardoli-Mahuva Road, Tarsadi,
Surat 394 350, Gujarat, India
Email: desaimadhavi30@gmail.com
*Corresponding author

S.V. Patel

MCA Department,
Sarvajanik College of Engineering and Technology,
R.K. Desai Marg. Opp. Mission Hospital,
Athwalines, Surat 395 001, Gujarat, India
Email: patelsv@gmail.com

Abstract: This paper presents a universal image steganalysis method based on feature selection by principal feature analysis (PFA). The goal of this paper is to increase the performance of existing image steganalysis approaches using PFA-based feature selection method and reduce the high dimensionality of the features used in state-of-the-art steganalysis methods. Principal component analysis (PCA) is widely used in pattern recognition applications. However, PCA has disadvantage that, all the generated features are transformed features. While, PFA selects the subset of preliminary features which contains necessary information. PFA is applied on spatial domain subtractive pixel adjacency matrix features and in case of transform domain, CHEN features (intra-block and inter-block Markov-based features) and CC-PEV features (PEV features enhanced by Cartesian calibration). The experimental results show that PFA is effective and efficient in eliminating redundant features. Experimental results prove that the use of PFA method in steganalysis is superior in terms of dimensionality reduction of features and increases the classification performance.

Keywords: Feature selection; high-dimensional feature; image steganalysis; image steganography; principal feature analysis.


Biographical notes: Madhavi B. Desai has received master degree from Gujarat Technological University and pursuing PhD from Uka Tarsadia University, Gujarat. Her areas of interest include pattern recognition, image processing, machine learning, and data mining.
1 Introduction

Secure communication is the most critical task in today’s digital world. Previously cryptography techniques were used for secret communication. All cryptography techniques encrypt original information in such a way that it becomes very difficult to interpret for third person. All cryptography techniques provide secrecy about the message being transmitted but it does not provide secrecy about the communication which is taking place between the source and the receiver. On the other side, steganography is a technique that hides the secret message into redundant bits of a cover media, i.e. video, audio, image and text. The basic aim of steganography is to keep the communication secret. Image is widely used on internet and it has a large number of redundant bits to hide, which makes it the most popular cover media for steganography. Clean image is known as a cover image and image with the secret message is known as a stego image. Visual properties of an image is preserved after embedding the secret message, then it is transferred through the internet or any public channel. There are many negative effects of an image steganography. Terrorists can use image steganography to communicate secretly. In addition to this, any important documents of the nation or company can be shared with the outsiders using image steganography. Porn images are also shared on the internet through image steganography techniques. That makes steganalysis an essential to counter against all these negative artifacts of an image steganography.

Many steganalysis techniques have been developed in the recent years, which can be partitioned into targeted and universal steganalysis. Targeted steganalysis focuses on breaking the particular or specific steganography method whereas universal steganalysis focuses on breaking wide variety of steganography techniques and it does not depend on any specific steganography method. Targeted steganalysis gives better performance compared to universal steganalysis techniques. Day-by-day upgradation in existing steganography methods and development of new steganography methods make universal image steganalysis more significant compared to targeted steganalysis. Steganalysis can be considered as a pattern recognition problem. It is divided in two parts. In the first part, features are extracted from the clean and stego images and then in the second part, classifiers are trained to identify images as clean or stego.

This paper focuses on reducing the high dimensionality of the features used in the state-of-the-art steganalysis methods. Performing feature subset selection in context of steganalysis offers several advantages as follows:

1. Computation time complexity is decreased for both feature extraction and training the classifier. Image steganalysis can be very useful in various real time applications where security is a major concern. The time required to detect the stego images is
PFA-based feature selection

Critical for real time applications. If we reduce the features then overall detection time can be reduced.

2 Irrelevant or redundant features are eliminated and essential features are kept to train the classifier.

3 Performance of any image steganalysis method does not depend on large dimensional feature set, but it depends on sensitive features which can detect the existence of hidden message in all different types of steganography techniques. That’s why feature subset selection enhances the performance of existing image steganalysis techniques.

The major outcome of this paper is to identify the most sensitive feature set which can clearly distinguish between clean and stego images. Rest of the paper is organised as follows. Section 2 highlights useful contributions made by researchers in feature extraction and feature selection. Proposed method using principal feature analysis (PFA) is explained in Section 3. Experimental setup and result analysis is presented in Section 4. Last section draws the concluding remarks of various experiments.

2 Related works

In recent years, considerable amount of research work is done for dimensionality reduction in steganalysis as pre-analysis to remove the irrelevant or redundant features and to keep the sensitive and important features. This process is mainly divided into two parts: feature extraction and feature selection. Feature selection is applied on the extracted features to select the most sensitive features from the candidate features. This section highlights the useful contributions made by various researchers in this domain.

2.1 Feature extraction

Based on whether an image contains a secret message or not, images are classified into clean images without secret message and stego images containing secret message. The crucial issue in feature extraction is to identify which type of features should be included in steganalysis process. Features should be sensitive to data hiding methods. Features should have more discriminative power to identify stego and clean class. Features should be general, i.e. features should be sensitive to all general data hiding methods not to specific method. Often it is very hard to achieve high recognition rate with single feature, so we need to make M-D feature vector.

In recent years, several feature extractors have been proposed on steganalysis to determine image as stego or clean. The following section highlights various popular feature extractors proposed by researchers in recent years

1 Farid and Lyu (2002) (72-D): This paper presented image steganalysis by detecting hidden messages using higher order statistics with support vector machine. Author extracted the statistical features formed by moments from three-level Haar wavelet subbands and prediction error image subbands. First four moments from each subbands and prediction error image subbands are extracted, which makes 72-D feature vector. Linear support vector machine and non-linear support vector machine is used for classification process. This method is tested against EzStego, Outguess,
JSteg and LSB steganography methods. It gives higher detection accuracy with higher embedding rate. Embedding rate indicates the size of message hidden in cover image. Non-linear support vector machine gives more classification accuracy than linear support vector machine.

2 Shi et al. (2005) (78-D): Image steganalysis method based on moments of characteristic function using wavelet decomposition and prediction error image and neural network is proposed in this paper. Statistical moments of wavelet characteristic functions are proposed to be used for steganalysis. Input test image is decomposed using three-level Haar wavelet decomposition. First three CF (characteristic function) moments from each wavelet subbands are extracted, that makes 39-D feature vector. These 39-D features are also extracted from the prediction error image. In this way total of 78-D features are proposed by the author. Neural network is used as a classifier. This paper claims that use of prediction error image enhances the detection accuracy of image steganalysis by reducing the effect caused by diversity of natural images (Shi et al. 2005).

3 CHEN (Chen and Shi, 2008) (486-D): Image steganalysis based on Markov features using inter-block and intra-block dependencies are proposed in this paper. Author has proposed the discrete cosine transform (DCT) domain steganalysis method. The transition probability matrix from each difference JPEG 2-D array utilising intrablock and interblock correlation are extracted as features. This makes total of 486-D feature vector. These features are given to Support Vector Machine (SVM) classifier for training and testing phase (Chen and Shi, 2008).

4 CC-CHEN (Kodovsky and Fridrich, 2009) (972-D): The major contribution of this paper is use of Cartesian calibration that enhances the features proposed by CHEN (Chen and Shi, 2008; Kodovsky and Fridrich, 2009).

5 Liu (2011) (216-D): The features of differential neighboring joint density are extracted from the absolute array of DCT coefficients between the original JPEG image and calibrated image to detect DCT-embedding based steganography. To detect the Yet Another Steganographic Scheme (YASS) steganography, the difference of neighboring joint density between candidate blocks and non-candidate blocks are calculated as features. SVM and logistic regression are used as classifiers. This paper demonstrates the use of difference of neighboring joint density function as features to break YASS steganography method (Liu, 2011).

6 CC-PEV (Chen and Shi, 2008; Pevny and Fridrich, 2007) (548-D): Merged Markov and DCT features (Pevny and Fridrich, 2007) are enhanced by Cartesian calibration and used for image steganalysis (Pevny and Fridrich, 2007).

7 Subtractive pixel adjacency matrix (SPAM, Pevny et al., 2010) (686-D): Image steganalysis by second-order Markov features and subtractive pixel adjacency matrix. This method is proposed to break LSB matching steganography. The difference between adjacent pixels is calculated from second-order Markov chain. The Markov transition probability matrices are calculated from horizontal, vertical, diagonal and minor diagonal difference matrix and combined to get 686-D feature vector (Pevny et al., 2010).
8 CC-C300 (Kodovsky and Fridrich, 2011) (48600-D): First high dimensional rich model for JPEG-steganalysis is presented in this paper. Concept of ensemble classifier is used by this paper. Family of weak classifier is built on random subspaces of pre-feature set. Final classifier is constructed by fusing the decisions of classifiers. The advantage of this approach is its universality, low complexity, simplicity and improved performance when compared to classifiers trained on the entire pre-feature set. Experiments with nsF5 and HUGO steganography algorithms demonstrate the usefulness of this approach (Kodovsky and Fridrich, 2011).

9 CF (Kodovsky et al., 2012) (7850-D): Compact rich model for JPEGs employing symmetrisation is used in this paper. The features are evaluated against three steganographic methods nsF5, MBS and YASS with different embedding rates (Kodovsky et al., 2012).

10 CC-JRM (Kodovsky and Fridrich, 2012) (22,510-D): Cartesian calibrated JPEG domain rich model, symmetries, both integral and DCT-mode specific features based image steganalysis method is presented in this paper. For a fixed steganographic channel, dimensionality of CC-JRM can be drastically reduced. Merging with spatial rich model further improves steganalysis. Cartesian calibration even helps in high dimensional subspaces (Kodovsky and Fridrich, 2012).

2.2 Feature selection

These techniques remove the redundant and irrelevant features from the whole extracted feature set. Feature selection process selects the subset of the original feature set by which same or comparable accuracy and less information loss can be obtained. In literature many authors have worked on feature selection process in steganalysis. Avcibas et al. (2003) has proposed the steganalysis method in 2001 using ANOVA feature selection method. In 2009, stego sensitive features selection using MBEGA was proposed by Geetha et al. (2009). Author has claimed that feature selection from state-of-art steganalysis methods using MBEGA can increase the performance. They have achieved average 60.17% feature reduction and decreased the computational cost. Feature selection methodology for steganalysis was proposed by Miche et al. (2006). In this approach, feature ranking is performed using a fast classifier called K-nearest neighbor. Dong et al. (2008) have proposed the blind image steganalysis using boosting the feature selection. Xia et al. (2012) proposed a methodology of feature selection using mutual information. By calculating co-variance between features and the embedding rate, Gul and Kurugollu (2011) established an evaluation indicator for each single dimension of the original feature set. After that, the original features are sorted according to their co-variance in the decreasing order. The best m-features are then determined and that subset of m-features is given as input to the classifier.

To reduce the dimensionality of feature vector, Fridrich et al. (2011) proposed method of ensemble classifiers. It consists of weak base learners which are constructed by randomly chosen subsets of the original features. The dimensionality of the each base learner is significantly smaller than the full dimensionality of the original feature set. The final decision is obtained by fusing the result of all base learners together under certain voting rule. Feature selection based on Fisher score in steganalysis was used by Lu et al. (2014). Using the Fisher criterion, separability of each of the single dimension feature is evaluated. Then starting from the first feature, as the dimension increases, the separability
of each component is analysed using Fisher criterion combined with Euclidian distance. Finally, the feature components with best separability are selected as the final features for steganalysis. Bee colony based feature selection algorithm for image steganalysis was proposed by Mohammadi et al. (2014). Artificial bee colony algorithm is inspired by honey bees’ social behavior in their search for perfect food sources. In this paper, classifier performance and dimensions of selected features are dependent on heuristic information for ABC and improved the performance of the classifier.

3 Proposed image steganalysis method

The performance of image steganalysis algorithm depends on sensitivity of the features against various image steganography methods. Figure 1 shows the steps for universal image steganalysis method based on effective feature selection. The efficiency of image steganalysis algorithm can be improved by selecting most sensitive features from given set of features. PFA is a feature grouping technique based on popular dimensionality reduction technique principal component analysis (PCA) (Jolliffe, 1986). PCA is an unsupervised approach to project the original features into low dimensional space. These selected low dimensional features are transformed features, not the subset of the original features.

Figure 1  PFA-based reduced dimensional universal image steganalysis method

As shown in Figure 1, features are extracted from training image dataset. SPAM (Pevny et al., 2010), CHEN (Chen and Shi, 2008) and CC-PEV (Pevny and Fridrich, 2007) feature extractors are used to extract features and these features are given to PFA. The selected features after PFA of clean and stego images are given as input to the classifier. During the training phase, known class and corresponding feature vector are given to the classifier. In the testing phase, unknown test images are taken as input which includes both clean as well as stego images. Features are extracted from test images and PFA is done on extracted features. The selected features are PFA on test images are passed as input the trained classifier. To evaluate the performance of PFA three sets of features are used and performance is compared for each of the three steganalysis methods. To further evaluate the results, experiments are carried out against stego images with variable
embedding rates and stego images generated using different data hiding methods. The following section describes basics of PCA and PFA.

3.1 Principal component analysis

Principal component analysis can be defined as orthogonal projections the data on to a lower dimensional linear space known as the principle subspace such that the variance of the projected data is maximised. The steps for PCA are as follows:

1. First, it constructs the $d \times d$ covariance matrix on the training vectors.
2. Then, eigenvalue and eigenvectors are calculated and sorted in decreasing order based on eigenvalues.
3. After this, $k$ eigenvectors corresponding to largest values are used as basis vector of subspace.
4. $K$-dimensional subspace vector $y$ is determined from the $D$-dimensional vector $x$ by following equation:

$$ y = A^T (x - \mu) $$

where $\mu$ is the mean of training vectors and $A$ is $d \times k$ matrix composed by the principal eigenvectors as columns.

3.2 Principal feature analysis

Principal feature analysis exploits the structure of principle component analysis. This method retains the maximum variability of features in low dimensional space and minimises the reconstruction error (Cohen et al., 2002).

Let $X$ be zero mean $n$-dimensional feature vector. Let $\Sigma$ denote covariance matrix of $X$ and $A$ be a matrix whose columns are orthogonal eigenvectors of the matrix $\Sigma$.

$$ \Sigma = AA^T $$

where $\Lambda$ is a diagonal matrix whose diagonal elements are the eigenvalue of $\Sigma$, $\lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \geq \lambda_n$. Let $A_q$ be the matrix of first $q$ columns of $A$ and let $V_1, V_2, \ldots, V_n \in \mathbb{R}^q$ be the rows of $A_q$. Each vector $V_i$ represents the projection of the $i$th feature (variable) of the vector $X$ to the lower dimensional space, that is, the $q$ elements of $V_i$ correspond to the weights of the $i$th feature on each axis of the subspace. The key idea behind the PFA is that the features which are highly correlated or have high mutual information will have similar absolute weight vector $V_i$ of features that are highly correlated and follow to choose one feature from each subset. The chosen features represent each group optimally in terms of high spread in the lower dimension, reconstruction and insensitivity to noise.

The algorithm of PFA is represented in following five steps:

1. Compute the sample co-variance matrix.
2. Compute the principle components and eigenvalue of the covariance matrix.
3. Choose the subspace dimension $q$ and construct the matrix $A_q$ from $A$. This can be chosen by how much variability of the data is desired to be retained. This retained
variability is the ratio between the sum of the first $q$ eigenvalue and the sum of all eigenvalue.

4. Cluster the vectors $|V_1|, |V_2|, ..., |V_q|$ to $p \geq q$ clusters using $K$-means algorithm. Euclidean distance is used as a distance measure for clustering algorithm.

5. For each cluster, find the corresponding vector $V_i$, which is closest to the mean of the cluster. Choose the corresponding feature, $x_i$, as a principal feature. This step will yield the choice of $p$ principal features. There are two main reason behind selecting the vector nearest to mean. This vector can be central feature of the cluster, the most dominant in it. Second reason behind this, it holds the least redundant information of features in other clusters. In this way, it satisfies both the properties required to achieve large ‘spread’ in lower dimensional space and good representation of the original data.

Clustering the representation of the features in the lower dimensional space. The complexity of the algorithm is of the order of performing PCA, because $K$-means clustering algorithm is applied on just $n_q$-dimensional vectors.

4 Experimental results and analysis

The experiments are performed to analyse the effectiveness of PFA in state-of-the-art steganalysis methods against various steganography methods. Standard BSDS300 (BSDSS300 Dataset: http://www.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/segBench) image database is used for the experiments: 200 images of training dataset and 100 images of testing dataset. Stego image database is created with F5 (F5: https://sourceforge.net/projects/vsl), LSB (F5: https://sourceforge.net/projects/vsl), dynamic battle stag (DBS, Digital Invisible Ink Toolkit, diit-1.5: http://diit.sourceforge.net), dynamic filter first (DFF, Digital Invisible Ink Toolkit, diit-1.5: http://diit.sourceforge.net), Blindseek (Digital Invisible Ink Toolkit, diit-1.5: http://diit.sourceforge.net), Blindhide (Digital Invisible Ink Toolkit, diit-1.5: http://diit.sourceforge.net) and StegHide (StegHide: http://steghide.sourceforge.net) steganography methods. Proposed PFA method of feature dimensionality reduction is evaluated against stego image datasets with different embedding rates of 1, 0.5 bpp. The stego image database using StegHide method is created with 0.05 bpp. Naive Bayes classifier is used for classification. Out of 200 training dataset, 70 images from cover dataset and 70 images from stego dataset are randomly selected for training the classifier. During testing phase, out of 100 images of testing dataset, randomly 30 images from cover and 30 images from stego are used. Quantitative evaluation of the proposed algorithm is done using confusion matrix as shown in Table 1.

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Confusion matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>True positive (TP)</td>
<td>False positive (FP)</td>
</tr>
<tr>
<td>False negative (FN)</td>
<td>True negative (TN)</td>
</tr>
</tbody>
</table>

TP: stego image is classified as stego image; TN: clean image is classified as clean image; FP: clean image is wrongly classified as stego image; FN: stego image is wrongly classified as clean image
Detection accuracy can be given by Eq. (3).

\[
\text{Detection accuracy} = \frac{TP + TN}{TP + FP + TN + FN}
\]  

(3)

Next section demonstrates various experiments on state-of-art steganalysis methods of spatial domain and transform domain.

4.1 Steganalysis with feature selection based on PFA

Penvy et al. (2010) proposed a steganalysis method to break the LSB matching steganography. In this approach, the differences between adjacent pixels are calculated using second-order Markov chains. Transition probability matrices are calculated on this difference matrix and subset of this transition probability matrix are used as features to break steganography method. It is found that a threshold value of 3 gives better performance. Finally, 343-dimensional Markov transition probability matrices obtained from horizontal, vertical, diagonal and minor diagonal neighboring pixel differences are computed and combined. That makes a total of 686-D SPAM features.

In first experiment, SPAM features are extracted from all of the cover images and stego images obtained using F5, LSB, DBS, DFF, Hideseek, Blindhide and StegHide steganography algorithms. PFA is applied on extracted features and finally reduced effective feature set is used for the steganalysis. Table 2 shows the detection accuracy of SPAM feature based universal image steganalysis algorithm against various data hiding methods with and without PFA based feature selection method.

<table>
<thead>
<tr>
<th>Embedding method</th>
<th>Embedding ratio (bpp)</th>
<th>Dimension of selected features</th>
<th>Reduction in feature set (%)</th>
<th>SPAM features</th>
<th>PFA selected SPAM features</th>
</tr>
</thead>
<tbody>
<tr>
<td>DBS</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>93.33</td>
<td>96.67</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>93.33</td>
<td>95</td>
</tr>
<tr>
<td>DFF</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>71.67</td>
<td>68.33</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>70</td>
<td>73.33</td>
</tr>
<tr>
<td>F5</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>95</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>96.67</td>
<td>96.67</td>
</tr>
<tr>
<td>LSB</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>95</td>
<td>93.33</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>95</td>
<td>93.33</td>
</tr>
<tr>
<td>Hideseek</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>95</td>
<td>96.67</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>93.33</td>
<td>96.67</td>
</tr>
<tr>
<td>Blindhide</td>
<td>1</td>
<td>138</td>
<td>79</td>
<td>95</td>
<td>95</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>138</td>
<td>79</td>
<td>90</td>
<td>88.33</td>
</tr>
<tr>
<td>Steghide</td>
<td>0.05</td>
<td>77</td>
<td>88</td>
<td>61.67</td>
<td>63.33</td>
</tr>
</tbody>
</table>
Table 2 shows the results of first experiment which demonstrates the effectiveness of PFA-based reduced dimensional features against various state-of-art steganography methods. As shown in Table 2 only 138 features are selected by PFA which reduces the original feature set by 80%. The results are taken against stego images obtained by various data hiding methods and different embedding rates. The results demonstrates that PFA based reduced feature set successfully breaks various steganography methods and achieves better results compared to original set of 686-D features.

Principal feature analysis finds sensitive features by comparing features before and after message embedding. If feature is sensitive enough to identify the changes imposed by the steganography methods even at low embedding rates it will be selected by PFA. If we get same feature dimensions for various embedding rates, then it suggests that the selected features after PFA are good enough to detect small changes imposed by the data hiding methods. That’s why even after changing the embedding rates same number of features are selected by PFA.

In order to check the generality of the PFA as feature reduction method, we applied PFA to transform domain features proposed by Chen and Shi (2008) and CC-PEV features (Pevny and Fridrich, 2007). Tables 3 and 4 show the performance comparison of transform domain image steganalysis methods with PFA selected features. The algorithm is evaluated against steganography methods like F5, LSB and StegHide with variable embedding rate.

### Table 3  Performance comparison between CHEN features (486-D) and PFA selected CHEN features against various steganography methods

<table>
<thead>
<tr>
<th>Embedding method</th>
<th>Embedding ratio (bpp)</th>
<th>Dimension of selected features</th>
<th>Reduction in feature set (%)</th>
<th>Detection accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CHEN features</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PFA selected</td>
</tr>
<tr>
<td>F5</td>
<td>1</td>
<td>138</td>
<td>71</td>
<td>98.76</td>
</tr>
<tr>
<td>F5</td>
<td>0.5</td>
<td>138</td>
<td>71</td>
<td>97.5</td>
</tr>
<tr>
<td>LSB</td>
<td>1</td>
<td>138</td>
<td>71</td>
<td>98.8</td>
</tr>
<tr>
<td>LSB</td>
<td>0.5</td>
<td>138</td>
<td>71</td>
<td>97.6</td>
</tr>
<tr>
<td>Steghide</td>
<td>0.05</td>
<td>77</td>
<td>84</td>
<td>54.86</td>
</tr>
</tbody>
</table>

Table 3 shows the performance of frequency domain features, i.e. CHEN features (Chen and Shi, 2008) against F5, LSB and StegHide methods after feature selection using PFA. PFA reduces original CHEN feature set by 85% and reduced 138-D feature set obtains same efficiency of classification. To further validate the results, experiment was carried out using another frequency domain feature set, i.e. CC-PEV. Total number of effective features that are obtained after applying PFA is 126-D which is 23% of original 548-D CC-PEV features. Total of 77% of features from CC-PEV are removed and only 23% most sensitive features after PFA are used for the further steganalysis process. As demonstrated by Table 4 PFA reduces original CC-PEV feature set by 77% and successfully achieves similar classification rate with only 27% original feature vector set.
Table 4  Performance comparison between CC-PEV features (548-D) and PFA selected CC-PEV features against various steganography methods

<table>
<thead>
<tr>
<th>Embedding method</th>
<th>Embedding ratio (bpp)</th>
<th>Dimension of selected features</th>
<th>Reduction in feature set (%)</th>
<th>Detection accuracy CC-PEV features</th>
<th>Detection accuracy PFA selected CC-PEV features</th>
</tr>
</thead>
<tbody>
<tr>
<td>F5</td>
<td>1</td>
<td>126</td>
<td>77</td>
<td>98.82</td>
<td>98.9</td>
</tr>
<tr>
<td>F5</td>
<td>0.5</td>
<td>124</td>
<td>77</td>
<td>97.7</td>
<td>97.8</td>
</tr>
<tr>
<td>LSB</td>
<td>1</td>
<td>122</td>
<td>77</td>
<td>99.2</td>
<td>99.2</td>
</tr>
<tr>
<td>LSB</td>
<td>0.5</td>
<td>123</td>
<td>77</td>
<td>98.8</td>
<td>98.85</td>
</tr>
<tr>
<td>Steghide</td>
<td>0.05</td>
<td>77</td>
<td>865</td>
<td>51.67</td>
<td>51.67</td>
</tr>
</tbody>
</table>

5  Conclusion

In this paper, an efficient universal image steganalysis method is proposed based on PFA algorithm. PFA is a feature selection method that is used to select most sensitive and effective features from set of popular spatial as well as frequency domain features. The results presented in Tables 2–4 clearly indicates that irrespective of feature types, data hiding methods and embedding rate, PFA efficiently selects most sensitive features from the dataset and increases the performance of existing steganalysis approaches. Experimental results demonstrate that more than 70% of redundant features are removed by PFA and similar accuracy is obtained with only 30% of remaining feature set. This paper proposes a strong feature reduction technique that can be used to reduce the feature dimension used for image steganalysis and achieve better detection accuracies with lower dimensional feature vector against various state-of-art steganography methods.

References


