DE GRUYTER OPEN

Journal of ELECTRICAL ENGINEERING, VOL 68 (2017), NO2, 117–124

Universal statistical steganalytic method

Martin Broda, Vladimír Hajduk, Dušan Levický *

Novel image steganalytic method used to detection of secret message in static images is introduced in this paper. This method is based on statistical steganalysis (SS), where statistical vector is composed by 285 statistical features (parameters) extracted from DCT (Discrete Cosine Transformation) domain and 46 features extracted mainly from DWT (Discrete Wavelet Transformation) domain. Classification process was realized by Ensemble classifier that was helpful in reduction of computational and time complexity. Proposed steganalytic method was verified by detection of popular image steganographic methods. Novel method was also compared with existing steganalytic methods by overall detection accuracy of a secret message.

K e y w o r d s: steganalysis, ensemble classifier, detection, DWT, DCT, statistical features

1 Introduction

In the field of secret message, there are several basic methods of steganography. The most popular are transformation techniques which transform cover media to transformation domain before the embedding process. The most popular transform ations are Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). For instance, among these techniques belong the algorithm F5 [1] and PQ [2]. Another method is called statistical steganography. Statistical steganography hides information in such a way that minimalizes statistical changes after an embedding process. Methods MB [3] or Outguess [4] can be denoted as statistical techniques of steganography.

On the other hand, there are several methods of steganalysis. Steganalysis is utilized to detect a presence of steganography system. The first method [5] is based on the extraction of statistical vector composed by 360 parameters, while the main part consists of Markov model statistical parameters from transition matrices. 120 parameters are extracted from the transition matrix and JPEG images are scanned not only by "zig-zag" form but also vertical and horizontal scanning are utilized. Thus the 360 parameters are the result of extraction. The classification into stego or cover object class was performed by CNPCA method (Class-wise Non-Principal Component Analysis) [6]. The second technique [7] utilizes DWT domain for the parameters extraction. As the parameters were chosen statistical moments of testing image characteristic functions also calculated for the prediction-version image between testing image and its predictable version. This method decomposes an image by 3-level DWT transformation with Haar wavelet function. The result is represented by 12 sub-bands. First three characteristic function moments of an image are calculated from whole image as well as individual sub-band to give 39 parameters. Additionally, if the calculation is performed for the predict image as well, resulting number of parameters is increased by another 39 parameters. It means that total length of a statistical vector is 78. This method utilizes neural networks to perform the classification.

In comparison to the previous mentioned methods, the presented steganalytic method extracts 285 parameters from JPEG domain and 46 from the domain after DWT transformation as well. It brings better detection of stego images and makes the algorithm more universal. Results of the detection process and comparison to the other methods will be presented in the section Experimental results.

2 Image steganalysis

The steganalysis is a field of information hiding and its primary function is detection of secret message in multimedia or detection of subliminal communication that is defined between two participants. If the process of steganalysis is able to reveal secret communication, steganographic system is defined as broken and purpose of steganography is defeated. Steganalytic method is defined as successful, when stego image can be differentiated from cover image with higher probability as a random guessing. Steganalysis can be supplemented by activity of extraction secret message's intelligence what requires a set of techniques for further analysis and increase of computational demands [8].

Universal statistical steganalytic methods are defined as set of detection techniques that are independent to the applied steganographic algorithm and achieve good detection results of embedded message that was hidden by new or unknown steganographic methods. The block diagram of such method is illustrated in Fig. 1. The model,

* Department of Electronics and Multimedia Communications, Technical University of Košice, Letná 9, 042 00 Košice, Slovakia, martin.broda, vladimir.hajduk, dusan.levicky@tuke.sk

DOI: 10.1515/jee-2017–0016, Print (till 2015) ISSN 1335-3632, On-line ISSN 1339-309X

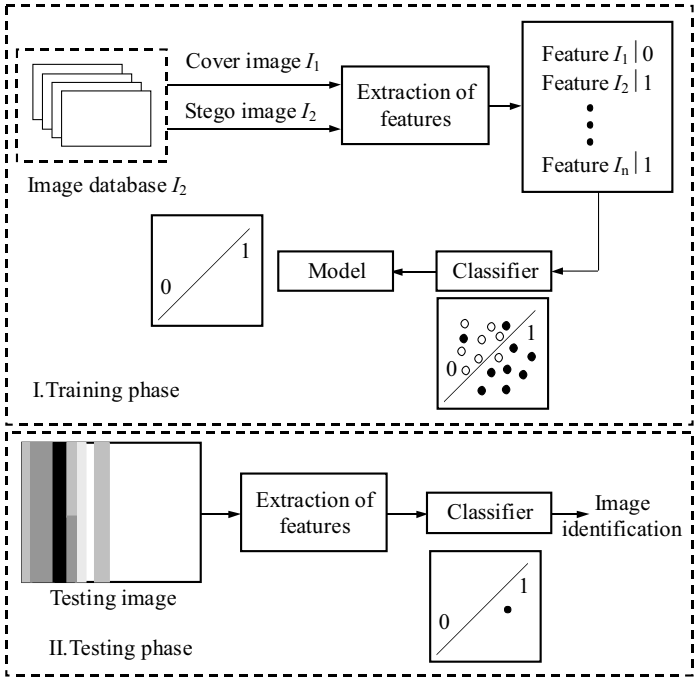

Fig. 1. Block diagram of universal statistical steganalysis

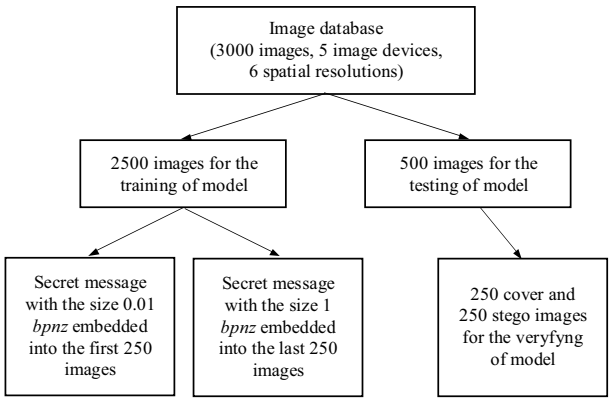

Fig. 2. The distribution of image database

result of the training phase, is formed by Classifier. Classifier finds the parameters of the separation hyper-plane using input statistical features extracted from cover and stego image database. The database consists of varied images marked by diverse steganographic techniques. The trained model is used during the testing phase. Classifier compares the extracted features from a testing image to determine whether it belongs to stego or cover class.

The main idea of steganalysis in static images is detection changes in statistic properties of cover image after embedding a secret message. Therefore, the calculation of those statistical features is very important in design of steganalytic method.

2.1 Statistical steganalysis

The Statistical Steganalysis (SS) was implemented altogether with calibration technique proposed by Fridrich [9]. The general model of image steganalysis contains a database of pre-selected natural images, specifically stego images and cover images, images without secret message. The database should include images created by a different imaging devices for the ensuring variety of images using different spatial resolutions, preprocessing, *etc.* The different types of statistical parameters from the spatial or the transformation domain are extracted from created image database. The selection of these parameters has a significant influence on the detection accuracy of secret message inserted by different steganographic algorithms. On the basis of these calculated features we can determine whether the verified image contains a secret message or not.

The basic part of the model training phase is based on the extraction of statistical features from the image database. This process can also include image calibration. The testing steganalytic method uses principle of images calibration that performs cropping of picture by 4 pixels in each direction. It results in image which has very similar statistical features as the cover image. The group of statistical parameters that were used in the extraction will be described in Subsection 2.3.

Each extracted statistical feature includes information identifier whether a given parameter is extracted from stego or cover image or even information about using steganographic method. This group of extracted statistical parameters is directed to classifier block. The aim of classifier is to separate the symptoms related to stego or cover image based on the associated information from the previous step. The result of this process is the trained model that is able to decide whether testing image includes secret message or not. Determining of steganographic method can be additional task in testing phase.

2.2 Image database

An important characteristic of the input image database is to ensure diversity in terms of use of different cameras, exposure and resolutions. Such diversity is important from the wide range of possible images coverage point of view.

Considering that the free image databases do not offer the necessary diversity, own input image database was created. Description of the image set distribution is shown in Fig. 2.

A database used for training of the various models included 3 000 still images created by 5 different image devices (3 conventional cameras and two mobile phones). The image resolution is in the range from 320×240 px to 192×1080 px. 2 500 images were selected for training phase of model and 500 images, unrelated to the images for the training, used for the model testing. In the next step, training set was divided into 10 subsets with 250 images, where secret message with different sizes were inserted into every subset using selected steganographic method. The same images without secret message were utilized as cover images in the training phase. Cover image database represented the second class for a classifier. 250 cover and 250 stego images were used for the verifying of trained model with specific steganographic method and secret message size. These images are different from images for the model training.

2.3 Statistical features

One of the most important part of the statistical steganalysis is represented by extraction of statistical parameters that are characterized by different values for stego and cover images. During the development of image steganalysis, researchers analyzed different ways of detecting secret messages in image data. The oldest methods used statistical parameters extracted from the spatial domain. This group can include features of binary similarity measures. These statistics provide good detection accuracy for known steganographic methods, especially secret message embedded in the spatial domain using LSB modification.

The steganalytic method proposed in [10] extracted 22 statistical features. As the classifier was used a method of Support Vector Machines SVM [11]. This method showed low detection accuracy for steganographic method using transformation domain (mainly Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT)) in the embedding process of secret message.

Therefore, research was especially focused on the selection of statistical features that would be suitable for a high detecting accuracy of secret messages embedded by popular steganographic method as F5, Outguess, MB and others, as well as the newly proposed algorithms using DCT and DWT domain. Proposed steganalytic method in this article includes 285 statistical features extracted from DCT domain (reasons for the selection of these statistical parameters and more details are stated in article [12, 13]) and 46 statistical features mainly from DWT domain. Proposed method in [13] provided low detection accuracy of secret message embedded using DWT domain steganographic method. It will be illustrated in the experimental results. Therefore, next statistical features extracted from DWT domain were integrated into the training of model.

Statistical features extracted from DCT domain (described in detail in [12, 13]) are:

- global histogram from all $64 \times n_B$ (total blocks of image) DCT coefficients and local histograms in mode $(i, j) \in \{(1, 2), (2, 1), (3, 1), (2, 2), (1, 3)\}$. The central part $\langle -5, 5\rangle$ of this histogram was selected due to maximum energy situated on this interval (66 statistical features).
- dual histogram (99 statistical features).
- functions of intra blocking dependencies of DCT coefficients — Variation (1 statistical feature).
- integral measures of intra blocking dependence (2 statistical features).
- functions from co-occurrence matrix $\mathbf{C}$ of neighboring DCT coefficients (25 statistical features).
- parameters of Markov model (81 statistical features).

The last 11 statistical features are based on inter blocking dependence. DCT image coefficients are divided into matrices with size $64 \times n_B$ and consequently there is calculated difference between adjacent blocks of DCT coefficients on equivalent positions.

$$D_{i,j} = d_{i,j} - d_{i,j+1} \tag{1}$$

where $D_{i,j}$ is matrix that is calculated by the difference between all adjacent blocks of DCT coefficients using horizontal sampling. Consequently, histogram (2) is defined from this matrix in interval $\langle -5, 5\rangle$, where is situated his maximum.

$$D = (D_L, \ldots, D_R) \tag{2}$$

where $L = \min_{i,j,k} d_{i,j}$ and $R = \max_{i,j,k} d_{i,j}$.

By this approach we obtain a statistical vector with the length 285 features extracted from DCT domain. As is shown in the section experimental results, this proposed statistical vector achieves very high detection accuracy for steganographic methods embedded the secret message in spatial or DCT domain, but the secret messages embedded by novel steganographic methods using DWT domain were detected with low detection accuracy.

Therefore, 46 new statistical features extracted mainly from DWT domain were added into statistical vector. Third level of 2D Haar discrete wavelet transformation (DWT) [7] is used for the extraction of statistical features in the proposed steganalytic method. $V_i(x, y)$, $H_i(x, y)$ and $D_i(x, y)$ represent detail coefficients of image in vertical, diagonal and horizontal direction while $A_i(x, y)$ expresses approximation coefficients of specific level.

First feature is image entropy before DWT decomposition. The next 36 statistical parameters are calculated from every direction of detail coefficients. The values of error signals define last 9 statistical features.

1) Image Entropy

$X_i,\ i = 1, 2, \ldots, N$ is random set. Its probability (1) p_i satisfies the condition

$$\sum_{i=1}^{N} p_i = 1\,, \quad 0 \le p_i \le 1\,, \quad i = 1, 2, \ldots, N\,. \tag{3}$$

Shannon entropy was defined as

$$H\left(p_1, p_2, \ldots, p_N\right) = -\sum_{i=1}^{N} p_i \log_2 p_i\,. \tag{4}$$

The difference between the image entropy corresponds to the visual differences between the images. Thus the image entropy is the attribute as image feature. The image stability trends to be determined based on entropy changes. Smaller entropy is more stable and clearer. When different pixels have equal probability, the entropy value is maximal.

2) DWT statistical features

On each layer of the wavelet decomposition coefficients, the mean value (5), variance (6), skewness (7) and kurtosis (8) of the sub-bands coefficients were calculated at each direction, whereby 36 statistical features (4 parameters*3 sub-bands*3 levels) were extracted.

$$E(x) = \frac{1}{n}\sum_{k=1}^{n} x_k\,, \tag{5}$$

$$\mathrm{Var}(x) = \frac{1}{n-1}\sum_{i=1}^{n}\big(x_k - E(x)\big)^2, \tag{6}$$

$$S(x) = E\left[\left(\frac{x - E(x)}{\sqrt{\big(\mathrm{Var}(x)\big)}}\right)^3\right], \tag{7}$$

$$K(x) = E\left[\left(\frac{x - E(x)}{\sqrt{\big(\mathrm{Var}(x)\big)}}\right)^4\right]. \tag{8}$$

3) Mean Square Error (MSE)

The goal of MSE measure is to compare two signals by providing a quantitative score that describes the degree of similarity or the level of error between them. Suppose that $x = \{x_i \mid i = 1, 2, \ldots, N\}$ and $y = \{y_i \mid i = 1, 2, \ldots, N\}$ are two finite-length, discrete signals (*eg* visual images), where N is the number of signal samples (pixels if the signals are images) and x_i and y_i are the values of the i^{th} samples in x and y, respectively [14]. The MSE between the signals is defined as

$$\mathrm{MSE}(x, y) = \frac{1}{N}\sum_{k=1}^{N}(x_i - y_i)^2\,. \tag{9}$$

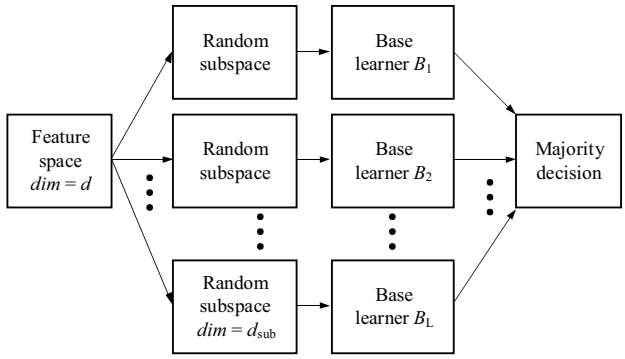

Fig. 3. Scheme of Ensemble Learning. Random subspaces are obtained from feature space dim and randomly and uniformly divided into each dsub

In our case, MSE was used as definition of error signal between approximation coefficients $A(n)$ and detail coefficients (horizontal, vertical and diagonal) in the same level of DWT decomposition. Decomposition coefficients of the same level are mutually correlated,

$$\mathrm{MSE}(A(n), S(n)) = \frac{1}{N}\sum_{k=1}^{N}\big(A(n)_i - S(n)_i\big)^2 \tag{10}$$

where $S(n) = \{H(n), D(n), V(n)\}\,,\ n = 1, 2, 3\,.$

The last 9 statistical features were obtained by this equation, because mean square errors were calculated for horizontal, diagonal and vertical detail coefficients and for all three levels.

2.4 Ensemble classifier

Next block in steganalytic scheme is classifier, where input of classifier is set of statistical features calculated in previous step. Result of classification process is the trained model between cover images and stego images that were obtained by specific steganographic method. Proposed steganalytic method in this paper utilizes Ensemble classifier.

Improved efficiency of individual classifiers is achieved by combination models, consisting of more individual classifiers. Classifier made by this technology is called Ensemble Classifier. Some techniques of combined models are Bootstrap Aggregation and Boosting.

1) Bootstrap Aggregation (bagging)

Ensemble classifier consists of many base learners B_L independently trained on a subset d_{sub} of feature dimensions dim of input cover and stego images (Fig. 3). Each base learner is a simple classifier working with (uniformly) randomly selected subspace of the feature space. In the testing phase, each base learner produces final decision whether testing subset of features belongs to cover or stego class. Final decision is made by aggregating of each minority decision [15].

This technique is known as bootstrap aggregation or bagging.

2) Boosting

Other method of combined learning is boosting. Boosting combine many weak learners (base learners) to make one strong with high accuracy. One of the earliest boosting frameworks is AdaBoost. AdaBoost, in comparison to bagging, trains individual base learners sequentially and every base learner focuses on samples that were more difficult to classify by previous base learners. The final decision is achieved by majority decision based on minority decisions of all base learners. This method achieves high accuracy and high efficiency of training time [15].

3 Experimental results

The first verification of the proposed steganalytic method used 285 statistical features from DCT domain and it was focused on comparison of two classifier types, specifically SVM with linear kernel function (L-SVM) and Ensemble classifier. From two ensemble methods mentioned in the section 2.4 we have decided for boosting. As base learners we used FLD classifier (Fisher Linear Discriminant analysis). Its detailed description is shown in [16]. FLD is a relatively simple classifier with fast algorithm appropriate to boosting method that uses weak learners to make a strong one.

Table 1. Comparison of detection accuracy for the SVM and Ensemble classifier

Testing algorithm	bpnz	L-SVM		Ensemble	
		TPR (%)	ACR (%)	TPR (%)	ACR (%)
F5	0.1	65.2	78.4	65.1	78.5
	0.25	94.4	92.5	93.7	92.6
	0.5	98.6	95.4	98.1	95.3
	1	100	98.5	100	98.2
MHF-DZ	0.1	64.5	61.9	65.1	61.7
	0.25	64.4	74.7	64.1	74.9
	0.5	70.6	79.9	70.6	78.7
	1	82.8	87.8	83.4	88.1
MB1	0.1	75.7	81.4	75.5	81.6
	0.25	90.4	93.3	90.1	92.4
	0.5	96.6	97.2	96.4	97.1
	1	100	98.9	100	98.4
MB2	0.1	84.4	83.2	84.6	82.1
	0.25	92.5	92.4	92.1	92.1
	0.5	98.1	94.5	98.4	94.9
	1	100	97.7	100	97.1
PQ	0.1	95.2	94.4	94.1	93.1
	0.25	94.3	97.5	94.7	95.4
	0.5	91.9	95.9	92.3	95.1
	1	92.7	95.1	93.4	95.9

This experiment verified detection accuracy of created models for 5 specific steganographic methods (F5, MHF-DZ, MB1, MB2 and PQ) - binary classification. The steganalyzer performance is highly susceptible to the size of secret message, which is denoted by bpnz (bit per nonzero AC DCT coefficients). The percentage value TPR (True Positive Rate) is expressed as true detection of stego images and the value ACR (Accuracy) is expressed as overall detection accuracy.

As is shown in the Tab. 1, the overall detection accuracy for the Ensemble classifier is very similar (small deviations in tenths of a percent) as in SVM classification system with a linear kernel function. The comparing of these classifiers showed the advantage of Ensemble classifier based on lower time of training process. Distribution of the set of statistical parameters into smaller units and the use of FLD reduced the computational and time complexity of the training model as is shown in the Tab. 2. The verification of training time was conducted on a sample of static images N^{trn} in number from 1 000 to 28 000, specifically for MB1 steganographic method.

The comparison of classifiers was realized by a computer with an Intel core i5 processor with a clock rate 2×2.5 GHz. As is shown in the Tab. 2, classification process of *eg* 12 000 static images, was taken 6 hours and 30 minutes for the SVM classifier and for the Ensemble classifier it decreased to 1 minute. These values reflect only the actual training time, not the time of the extraction of statistical parameters, which also takes some time depending on the computational complexity of extracted statistical features. These results show that using of Ensemble classifier in the proposed steganalytic method with specific size of statistical vector is highly effective.

Table 2. The comparison of training time for SVM and Ensemble classifier

N^{trn}	SVM (training time)	Ensemble (training time)
1 000	2 m	5 s
2 000	11 m	< 30 s
400	38 m	30 s
8 000	2 h 49 m	< 1 m
12 000	6 h 30 m	1 m
16 000	13 h	1 m 18 s
20 000	–	1 m 43 s
28 000	–	2 m 14 s

Proposed image steganalytic method have extracted 285 statistical features from DCT domain and it was verified by two steganographic methods using DWT domain for the embedding of the secret message [17, 18]. As the results show in the Tab. 3, designed steganalytic method extracted 285 statistical features from DCT domain only provides worse results for the detection of steganographic methods embedded secret message in the DWT domain as previously verified methods using DCT domain.

Table 3. The comparison of detection accuracy for statistical steganalysis with vector length 285 (only DCT features) and 285+46 (DCT + DWT features) statistical features

Verified methods	bpp	SS (285)		SS (285 + 46)	
		TPR (%)	ACR (%)	TPR (%)	ACR (%)
Wavelet Stego [17]	0.05	65.2	67.4	92.4	91.4
	0.1	68.4	69.5	96.1	96.8
	0.2	73.2	72.3	99.1	98.8
	0.3	78.1	75.6	100	99.1
Proposed method DWT [18]	0.05	63.1	62.9	89.9	89.4
	0.1	65.4	64.5	94.1	94.4
	0.2	70.4	69.9	95.9	96.1
	0.3	73.4	71.2	98.1	97.8

Table 3 shows the value of a successful detection of stego images TPR and the overall detection accuracy ACR for the steganalytic method extracted a set of 285 statistical features from DCT domain (SS (285)) and statistical steganalytic method with the addition of features extracted mainly from DWT domain (SS (285+46)) after application of the Haar functions. These all extracted statistics are explained in more details in Subsection 2.3. Two steganographic methods used for embedding secret message using modification of transform coefficients in specific level of two-dimensional DWT were selected for the verification of proposed steganalytic methods.

The first testing steganographic method is marked as "WaveletStego" where image is firstly transformed into the Haar DWT domain. Next, the secret message is reorganized into a string of bits using Huffman coding. Subsequently, each bits' triplet of that Huffman code (*eg* 000 to 111) is selected and inserted instead of the three lowest bits of sub-band coefficients in the selected cover image obtained by 2D Haar DWT. Subsequently, inverse DWT is applied to these modified sub-band, whereby an image with an embedded secret message is obtained. This method is further described in [17].

The second of the testing steganographic methods is own designed method [18], also working in DWT domain. This method is based on embedding of text into colorful static images and it also solves lossless conversion between RGB and YC_bC_r models if secret message is embedded into the chrominance component C_b. This component was chosen because of the smallest impact on perceptive imperceptibility after inserting of the secret messages. Cb component is not modified directly, but it is transformed using 2D Haar DWT. Subsequently, the LSB bits of the sub-band HH (alternatively also the sub-bands HL and LH) is modified by bits of the secret message. This method is further described in [18].

The both steganographic methods were tested for two lengths of statistical vector used in the process of steganalysis. Verification were realized for different sizes of inserted secret message expressed by parameter bpp (*bits per pixels*). This parameter expresses the number of secret message bits relative to the total number of image pixels. The comparison of detection accuracy was realized for statistical steganalytic method which extracted 285 statistical parameters (SS (285)) from DCT domain and statistical vector with previous features plus 46 new features (SS (285+46)) mainly extracted from Haar DWT domain. As is shown in the Fig. 4, better results are achieved by statistical vector SS (285+46), where the selected statistics are able to capture the changes carried out in DWT transform coefficients.

The comparison of steganographic methods shows that higher detection accuracy was obtained for the detection of "WaveletStego" method. The previously proposed DWT method had advantage especially in the small sizes of secret message, where was achieved the distraction of secret messages in the image by using AES encryption. It makes the detection process more complicated.

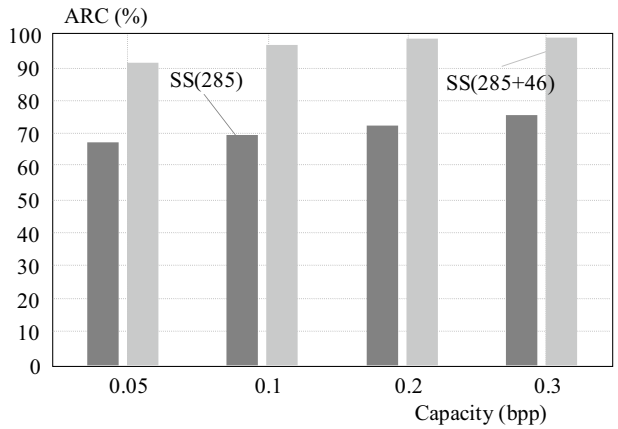

Fig. 4. The ACR comparison of statistical vector SS (285) and SS (285+46) in image steganalysis for the steganographic method WaveletStego

The next verification of proposed steganalytic method was focused on its comparison with existing image steganalytic methods. Proposed method used an Ensemble classifier and statistical vector with the length SS (285+46) was compared with current image steganalytic methods published in [5] and [7].

The first compared method [5] is based on the extraction of statistical vector with the length 360, while the main part consists of Markov model statistical parameters from transition matrices. The classification into stego or cover object class was performed by CNPCA classifier [6]. The second compared method [7] uses a DWT domain for the extraction of statistical parameters. As parameters were used statistical moments of the characteristic functions in the verified images. They were also calculated for version expressed prediction-error image between the test image and its predicted version. In this method, overall length of statistical vector is 78 features and neural networks were used as a classifier.

The comparison detection accuracy results (ACR) of the proposed method SS (285+46) and existing methods

are illustrated in Tab. 4. The proposed image steganalytic method SS (285+46) and described existing methods were verified by four selected steganographic methods F5, Outguess, MB and JPHS. The size of an embedded secret message was expressed by parameter bpnz.

Results show that the proposed method SS (285+46) reaches in most cases better ACR as the other steganalytic methods. However, a secret message embedded by steganographic method MB (Model-Based) was detected with higher accuracy using method from Xuan *et al* as the proposed method. This was caused since the MB method is especially detectable using statistics from Markov model and currently method from Xuan *et al* is based on extraction of these features.

Table 4. The comparison of the proposed steganalytic method SS (285+46) with existing methods

Verified methods	bpnz	Xuan *et al* [5]	Shi *et al* [7]	SS (285+46)
		ACR (%)	ACR (%)	ACR (%)
F5	0.25	74.6	61.4	75.1
	0.4	84.3	69.4	91.4
	0.6	94.3	72.1	98.5
	0.8	95.4	78.4	99.1
Outguess	0.05	71.2	54.1	76.1
	0.1	91.4	64.3	94.1
	0.15	93.1	70.1	95.9
	0.2	97.9	74.9	97.9
	0.25	96.4	78.9	98.1
	0.4	97.9	81.2	98.6
MB	0.1	84.1	53.4	85.4
	0.2	96.4	59.6	94.6
	0.4	99.1	65.9	98.9
	0.6	99.4	69.7	98.9
	0.8	99.7	74.4	98.9
	1	99.7	78.6	98.9
JPHS	0.1	75.4	59.5	76.1
	0.25	81.4	64.1	89.1
	0.4	87.6	66.9	89.4
	0.5	87.9	71.2	92.1
	0.6	90.4	73.4	94.3

The lowest detection accuracy was achieved by method from authors Shi *et al*, since this method is only based on extraction of statistical features from DWT domain which do not provide sufficient detection accuracy of steganographic methods which utilize DCT or JPEG domain. This property shows also other available techniques using the limited parameters from the DWT domain which are more mentioned in [19].

This verification confirmed the known property that the detection accuracy is increased with the enlarging of the secret message size for all steganographic methods. The comparison of the overall detection accuracy (ACR) of steganographic method F5 for three verified steganalytic methods is illustrated in other way in the Fig. 5.

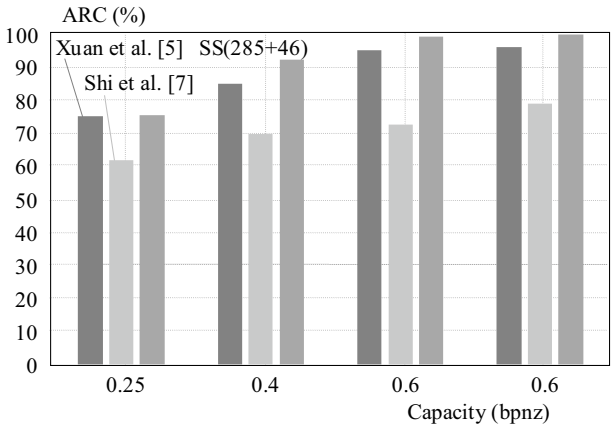

Fig. 5. The comparison detection accuracy of steganographic method F5 for three steganalytic methods

4 Discussion

On the basis of experimental results, it can be pronounced that the better way is a chosen of Ensemble classifier rather than L-SVM due to much faster computational algorithm and comparable efficiency. An adding of the 46 characteristic features extracted from DWT domain caused higher steganalyzer accuracy of the testing steganography algorithms. The comparison of the verified steganalytic methods from the previous section shows that a higher length of statistical vector does not always guarantee a higher detecting success rate of secret messages. Method from Xuan *et al* extracts 360 features, but it achieves lower detection accuracy for 3 of 4 verified steganographic methods than the proposed method. An important characteristic is the selection of those statistical features that clearly expresses the difference between the image version with and without secret messages in order to avoid false assignment in the classification.

5 Conclusion

In this paper, we proposed the novel image steganalytic method that combines features extracted from DCT (285 statistical parameters) and DWT domain (46 statistical parameters). The aim of research was proposed steganalytic method that will be able to detect steganographic methods that are based on the modification transform coefficients in DCT and/or DWT domain. The proposed method SS (285+46) was compared with existing steganalytic method. Results show that the proposed method SS (285+46) reaches better detection accuracy as existing steganalytic methods from Xuan *et al* and Shi *et al* in most cases. The comparison of testing methods proves that a higher number of statistical vector does not always guarantee a higher detection accuracy of secret

messages. Ensemble classifier is used in classification process, since it reduces time and computational complexity as is shown in experimental results.

Acknowledgements

This publication arose thanks to the support of the Operational Programme Research and development for the project "(Development of the Centre of Information and Communication Technologies for Knowledge Systems) (ITMS code 26220120030), co-financed by the European Regional Development Fund" (50%) and Ministry of Education of Slovak Republic VEGA Grant No. 1/0075/15 (50%).

References

[1] A. Westfeld, "F5-A Steganographic algorithm: High capacity despite better steganalysis", *Proceedings of the 4th International Workshop on Information Hiding*, New York Springer-Verlag, 2001, pp. 289-302. ISBN 3-540-42733-.

[2] J. Fridrich, M. Goljan and D. Soukal, "Perturbed quantization steganography", *Multimedia Systems Journal*, 2005, vol. 11, no. 2, pp. 98-107. DOI 10.1007/s00530-005-0194-.

[3] P. Sallee, "Model-based methods for steganography and steganalysis", *International Journal of Image and Graphics*, 2005, vol. 5, no. 1, pp. 167-190. ISSN 1793-675.

[4] N. Provos, "Defending against statistical steganalysis", *Proceedings of the 10th USENIX Security Symposium*, Washington, DC USENIX Association Berkeley, 2001. ISBN 978-1-931971-23.

[5] G. Xuan *et al* "JPEG Steganalysis based on classwise non-principal components analysis and multi-directional Markov model", *Proceedings of the 2007 IEEE International Conference on Multimedia and Expo*, pp. 903-906. DOI 10.1109/ICME.2007.428479.

[6] G. Xuan *et al* "A novel pattern classification scheme: classwise non-principal component analysis (CNPCA)", *18th International Conference on Pattern Recognition (ICPR)*, Hong Kong, 2006, vol. 3, pp. 320-323. DOI 10.1109/ICPR.2006.14.

[7] Y. Q. Shi *et al* "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network", *Proceedings of the 2005 IEEE International Conference on Multimedia and Expo*, Amsterdam, Netherlands. DOI 10.1109/ICME.2005.1521412.

[8] R. Bohme, "Advanced statistical Steganalysis", *Dresden*, Springer 2009. ISBN 978-3-642-14312-.

[9] J. Fridrich, M. Goljan and D. Hogea, "Steganalysis of JPEG images, Breaking the F5 algorithm", *Information Hiding*, 5th International Workshop, vol. 2578 of Lecture Notes Computer Science, pp. 310-323, Noordwijkerhout, Netherlands Springer-Verlag, 2002. DOI 10.1007/3-540-36415-3_2.

[10] I. Avcibas, M. Kharrazi, N. Memon and B. Sankur, "Image Steganalysis with binary similarity measures", *EURASIP Journal on Advances Signal Processing*, 2005. DOI 10.1155/ASPP.2005.274.

[11] S. R. Gunn, "Support Vector Machines for Classification and Regression", *Southampton. University of Southampton*, Faculty of Engineering, Science and Mathematics, 1998. Available at http//users.ecs.soton.ac.uk/srg/publications/pdf/SVM.pd.

[12] V. Bnoci, M. Broda, G. Bugr and D. Levick, "Universal Image Steganalytic Method", *Radioengineering Journal*, vol. 23, no. 4, pp. 1213-1220, 2014. ISSN 1210-251.

[13] G. Bugár, V. Bánoci, M. Broda and D. Levický, "A Novel Approach for Image Steganalysis", *Proceedings of ELMAR-2014 56th International Symposium*, Zadar, Croatia, Zagreb University of Zagreb, Faculty of Electrical Engineering and Computing, 2014, pp. 171-174. ISBN 978-953-184-199-.

[14] Z. Wang and A. C. Bovik, "Mean Squared Error: Love It or Leave It? A new look at signal fidelity measures", *IEEE Signal Processing Magazine*, vol. 26, no. 1, pp. 98-117, 2009. DOI 10.1109/MSPP. 2008.93064.

[15] 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, 2012. DOI 10.1109/TIFS.2011.217591.

[16] M. Welling, "Fisher Linear Discriminant Analysis", *Department of Computer Science*, University of Toronto. Available at http//www.ics.uci.edu/ welling/classnotes/papers_class/Fisher-LDA.pd.

[17] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", *International Journal of Computer Science and Security (IJCSS)*, 2011, vol. 4, no. 6, pp. 561-570. ISSN 1985-155.

[18] M. Broda, V. Hajduk and D. Levický, "Image Steganography Based on Combination of YCbCr Color Model and DWT", *Proceedings of ELMAR-2014 57th International Symposium*, Zadar, Croatia, Zagreb University of Zagreb, Faculty of Electrical Engineering and Computing, 2015, pp. 201-204. ISBN 978-953-184-209-.

[19] M. Ashraf and M. Mahmoud, "Performance Evaluation of Different Universal Steganalysis Techniques JPG Files", *Annales UMCS*, Informatica, 2013, vol. 12, no. 3, pp. 121-139, ISSN (Online) 2083-3628, ISSN (Print) 1732-136.

Received 23 December 2016

Martin Broda was born in Prešov, Slovakia in 1988. He received his (MSc) degree from Faculty of Electrical Engineering and Informatics, Technical University in Košice. Nowadays, he is a recent graduate of PhD study at Department of Electronics and Multimedia Communications, focusing on multimedia security, image steganography, steganalysis and digital watermarking.

Vladimír Hajduk was born in Košice in 1990. He received his (MSc) from Faculty of Electrical Engineering and Informatics, Technical University in Košice. Nowadays, he is a PhD student at Department of Electronics and Multimedia Communications. His research interests include image steganography, steganalysis and image processing.

Dušan Levický was born in 1948 in Slanec, Slovakia. He received the (MSc) degree at the Faculty of Electrical Engineering at the Technical University in Košice in 1973. The (PhD) degree received in 1985 in the field of electronics. In 1986-2012 he was the head of Department of Electronics and Multimedia Communications. In this time is full professor at the Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interests include multimedia communications, image coding, applied cryptography, digital image watermarking and steganography."