New Blind Steganalysis Framework Combining Image Retrieval and Outlier Detection

Yunda Wu, Tao Zhang, Xiaodan Hou and Chen Xu
Zhengzhou Information Science and Technology Institute
Zhengzhou, Henan 450002 - P. R. China
[e-mail: {yunda_wu, brunda, hxd2305}@163.com]
[e-mail: xuchenxd@126.com]
*Corresponding author: Tao Zhang

Received May 7, 2016; revised October 11, 2016; accepted November 15, 2016; published December 31, 2016

Abstract

The detection accuracy of steganalysis depends on many factors, including the embedding algorithm, the payload size, the steganalysis feature space and the properties of the cover source. In practice, the cover source mismatch (CSM) problem has been recognized as the single most important factor negatively affecting the performance. To address this problem, we propose a new framework for blind, universal steganalysis which uses traditional steganalyst features. Firstly, cover images with the same statistical properties are searched from a reference image database as aided samples. The test image and its aided samples form a whole test set. Then, by assuming that most of the aided samples are innocent, we conduct outlier detection on the test set to judge the test image as cover or stego. In this way, the framework has removed the need for training. Hence, it does not suffer from cover source mismatch. Because it performs anomaly detection rather than classification, this method is totally unsupervised. The results in our study show that this framework works superior than one-class support vector machine and the outlier detector without considering the image retrieval process.

Keywords: Blind steganalysis, Image retrieval, Outlier detection

1. Introduction

Modern steganalysis can be incredibly sensitive and accurate [1][2], but only in the condition that the steganalyst has access to embedding algorithm, payload size and the cover source used by the steganographer. It is perfectly reasonable for laboratory conditions, but not very realistic for the steganalysis application in the real world. Once the detector has no information about the embedding details applied by the steganographer, there is a great chance that the detection performance will degrade [3][4][5], often dramatically. This condition inevitably results in the so-called model mismatch problem. Only a few publications have tested steganalysis in such scenario.

The most frequently used method dealing with algorithm mismatch was one-class support vector machine (OC-SVM) which was first introduced in [6]. As OC-SVM only requires the training cover images, the classifier can contend with novel and yet unknown stego methods [7]. However, stego image with relative low payload is much harder to detect and the accuracy might be random guessing if it suffers from cover source mismatch.

There are several solutions to mitigate the cover source mismatch. It is generally considered that simple classifiers may be more robust to variations between training and testing data. The papers [4][8] proposed to use the "Large Data" approach combined with simple classifiers such as perception or ensemble classifier, which requires the training data set as large and diverse as possible.

Pevný *et al*. [4] and Cancelli *et al*. [9] investigated the difference of detection performance in single and heterogeneous image database. Pevný et al proposed a strategy using an image pre-classification method and such strategy provides significant guidance to the practicability of this algorithm.

Inspired by Pevný's work, another approach called forensics-aided steganalysis is investigated in [10][11][12]. A bank of steganalyzers are first trained based on source identification, tampering detection, image content or other characteristics of images type. The image under investigation is analyzed and sent to the corresponding steganalyzers. The detection performance has a great improvement but only at the cost of huge computation complexity and training many classifiers. Besides, the detector fails in the condition when a sample does not belong to any image type available.

Cho *et al*. [13][14] did some researches a step further. They partitioned or segmented the test image into several smaller homogenous blocks before pre-classification according to statistical properties. The steganalysis of the whole image can be conducted by fusing steganalysis results on all blocks. The block-based image steganalysis was shown to have better performance but still suffering from high computational complexity.

Li *et al*. [15] introduced the transfer learning algorithm in machine learning to the blind detection field. They derived new representations from original features for training and testing samples by generalized transfer component analysis to correct the mismatches. However, this method requires that the training and testing sources should be close, which is hardly satisfied in the in the realistic steganalysis application.

The above-mentioned detection methods investigate mismatch problem from multiple perspectives. However, none of them considers both embedding algorithm mismatch and cover source mismatch simultaneously. Most of the methods still need to train. Recently, Ker et al. presented a new approach in this direction and did some promising researches. Firstly, they proposed a novel paradigm for steganalysis based on clustering rather than classification in [16]. It judges the behavior of the test actor by assuming that most of the actors are innocent. As there is no need for training and information about the embedding algorithm, this method is

totally blind and universal. This problem was further studied in [17][18]. The authors conducted the experiment in a new, highly realistic dataset. In addition, the hierarchical clustering method was replaced by local outlier factor (LOF) which performs much better. It is noteworthy that all of these methods focus on the actors rather than the individual transmitted objects. It may fail when there is none or multiple guilty actors. What's more, this approach was not consistent with the purpose of detecting the actual hidden message. It is necessary to identify the single image in most cases. As the single test object is more easily affected by the difference in cover source than embedding, this method is no longer valid when we directly migrate it to the individual image steganalysis.

To solve the aforementioned problems, we propose a new framework for steganalysis combining the image retrieval and outlier detection. All features suitable for blind detection can be applied to this framework and it is the single object rather than the actors investigated in our method. For a given image, cover images with similar statistical properties are searched from the massive cover image dataset to establish an aided sample set. A test set is composed of the test image and its aided sample set. Then, the framework performs outlier detection on the test set to determine the type (cover or stego) of the test image. The results in our study shows that this framework behaves better than one-class support vector machine and the outlier detector without considering the image retrieval process.

The rest of the paper is organized as follows: Section 2 introduces the steganalysis framework proposed in this study, the general techniques of source camera identification and outlier detection. Section 3 describes the experiment setup employed to evaluate the proposed framework. Section 4 presents the experiment results and parameter selection. In Section 5, the paper concludes and provides the possible directions for future research.

2. Proposed Framework

2.1 Motivations

In reality, one cannot normally acquire training images from the exact cover source, thus resulting in the model mismatch problem. But with the help of large amount of data available in the internet, it is feasible to search images with similar characteristics to mitigate the mismatch as much as possible. For a given image, cover images with similar statistical properties are searched from the reference dataset to establish an aided sample set. The reference database can be some specific image databases or the vast diversity images downloaded from the social network. We combine the test image and its aided samples into a test set. Outlier detection is then performed on the combined dataset to determine the type of the given test image.

2.2 Camera Source Identification

Images from similar source have less mismatches and it is obvious that there is a great difference between different camera models. Based on this fact, different camera models are commonly used in the papers [16][19][20][21] to represent different actors or the cover source mismatch scenarios. We can mitigate the mismatch impact if we know the source of the test image. Inspired by this idea, we try to identify the source of the digital camera images.

As one of the common-known digital image forensic problem, source camera identification (CSI) has received plenty of attention in the past few years. Several approaches have been proposed to identify the source of an image and there are mainly two branches. One is to identify various brands and models [22][23]; the other is to identify the exact camera taking

this image [24][25]. In steganalysis, images from the same device are considered from the same source. But in the total cover source imsmatch scenarios, it is impossible to recongnize the exact same device. We choose the first approch and consider the images from the same camera as from the same source. The camera model identification technique proposed by Shang Gao [26] is adopted in this paper which requires only linear filtering operation.

Typical digital cameras capture color images with a single sensor and an array of filters. The color filter arrays (CFA) are placed before sensors to filter the wavelengths of the light that can reach each sensor. As a result, the sensors record only one color value at each pixel location. After the CFA color sampling, the remaining color components are recovered by CFA interpolation (also known as demosaicing). Different camera manufactures or models possibly use different CFA pattern and interpolation algorithms. The underlying structure of the color filter arrays and the demosaicing algorithm can reflect the model difference to some degrees, which can be used in camera model identification.

Due to the CFA sampling and interpolation process, the full color image is combined of originally recorded and the interpolated pixels. The difference of interpolation characteristics can be reflected from the ratio of statics between recorded part and the estimated part. However, the source pattern of the test image is unknown in camera model detection. This problem is solved by calculating above estimation ratio under several common hypothesis CFA patterns. What's more, because the camera-specific statistics is easily affected by image content, the features are extracted from image sensor noise rather than original image data. The noise residual is calculated by subtracting the denoised image from the original one. The de-noising filter F is from [27]. The features are calculated as follows:

$$\max\left(\frac{stat(N_{p_i}^r)}{stat(N_{p_i}^e)}, \frac{stat(N_{p_i}^e)}{stat(N_{p_i}^r)}\right) \quad i = 1, \ldots, n, \tag{1}$$

Where $N_{p_i}^r$ and $N_{p_i}^e$ denote raw and estimated part of image noise under the *i*th hypothesis CFA pattern, *stat*() denotes statistics extraction method. Finally, 69-D features will be extracted from every image. The detailed algorithm can be found in [26].

2.3 Outlier Detection

With more and more data are collected and stored, there is a growing interest in the detection of abnormal or suspicious patterns in large data. By conducting a comparative evaluation of the outlier detection methods on real-world datasets, the authors [28] have demonstrated that LOF and SVDD perform best among several prevalent outlier methods. Because LOF is easy to implement and the only parameter need to be specified is the number of nearest neighbors, it is more suitable for unsupervised classification. The detailed description is given below:

For a specific object *p*, we get its *k* nearest neighbors $N_k(p)$ and they satisfy that

$$N_k(p) = \{q \mid d(p,q) \le dist_k(p)\}, \tag{2}$$

Where $d(p,q)$ is the Euclidean distance between *p* and *q*. $dist_k(p)$ is the distance from *p* to its *k*th nearest neighbor. In this study, *k* refers to the recommended value by [29], that is, *k*=10.

The reachability distance of object *p* from *q* is defined as:

$$d\_reach(p,q) = \max\{dist_k(q), d(p,q)\}. \tag{3}$$

Then we get the local reachability density $lrd_k(p)$ of p,

$$lrd_k(p) = \frac{k}{\sum_{q \in N_k(p)} d\_reach(p,q)}. \tag{4}$$

Finally, the local outlier factor (LOF) of p is

$$lof_k(p) = \frac{1}{k} \sum_{q \in N_k(p)} \frac{lrd_k(q)}{lrd_k(p)}. \tag{5}$$

The object lying deep inside a cluster will have a neighborhood density equal to its neighbors, so the LOF value will be around 1. On the contrary, the object far away from its neighbors will have a relative higher local outlier factor. In the application of steganalysis, if a test image is a cover image, we expect it would not deviate from the rest otherwise it will be identified as a stego image.

2.4 Procedure of the Proposed Framework

We have described the overall mechanics of the proposed framework in Section 2.1. To be specific, we retrieval images based on source camera identification and conduct outlier detection by LOF in this study.

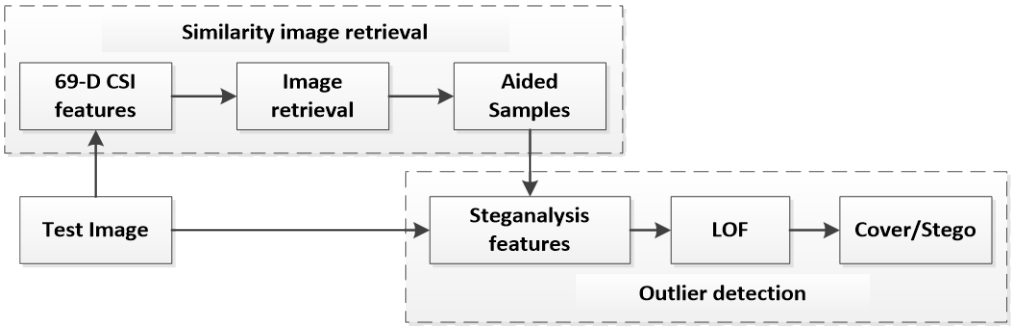

Fig. 1. Structure of the proposed framework

The structure of the proposed framework is illustrated in **Fig. 1**. And the steganalysis procedures are as follows.

(1) For a test image, the retrieval features based on characteristic of CFA and interpolation are extracted. The feature distances between the test image and the images in the reference database are calculated.

(2) From the reference database, we retrieve images by selecting the K (number of aided samples) nearest neighbors of the test image based on feature distance. The test image and its corresponding aided samples combine a whole test set.

(3) We perform LOF on steganalysis features of the test set to determine whether the test image is a cover or stego. The detector assumes that the majority of the images are innocent and tries to identify stego image as an outlier. However, ensuring that the stego image has the highest LOF value is actually unrealistic. The test image will be verified to be an outlier only if its LOF value is in the top n list.

3. Experimental Setup

3.1 Image Database

Our experiments use the "Dresden image database" [30] which is composed of over 14000 images acquired under controlled conditions by 73 cameras from 25 different models. As we have mentioned before, the images from same camera model are considered from the same source. In the experiment, only the images taken from more than one device per model were selected for model detection. We chose 10 camera models with the most images quantities total of 10248 from 42 different devices as our image database. **Table 1** summarizes the original properties of selected models and the number of corresponding devices and images. All the images would be centrally cropped to the size of 1024x1024 to avoid the influence of various image sizes. For the source identification purpose, we did not convert the color image into gray scale as usual.

Table 1. Camera models used in this research

NO.	model	Device num/model	Image num/model	Native resolution	Image format
1	Kodak_M1063	5	2391	3664x2748	JPEG
2	Nikon_CoolPixS710	5	925	4352x3264	JPEG
3	Nikon_D200	2	751	3872x2592	JPEG
4	Olympus_mju_1050SW	5	1040	3648x2736	JPEG
5	Panasonic_DMC-FZ50	3	931	3648x2736	JPEG
6	Praktica_DCZ5.9	5	1019	2560x1920	JPEG
7	Ricoh_GX100	5	854	3648x2736	JPEG
8	Samsung_L74wide	3	687	3072x2304	JPEG
9	Sony_DSC-T77	4	725	3648x2736	JPEG
10	Casio_EX-Z150	5	925	3264x2448	JPEG

3.2 Steganographic Algorithms and Steganalysis Features

Three steganographic algorithms are employed in our experiment: nsF5, MB1 and MB2. To simplify the problem, all the hidden messages are embedded in the first component of the color image DCT coefficients. Payload is measured in bits per non-zero AC coefficient (bpnc). For steganalysis, we simply choose PF274 features [31]. It can reliably detect the steganographic algorithms used above. Compared with modern rich features, they have good signal to noise ratio and the extraction is much faster. Correspondingly, all the features are extracted from the first component of DCT coefficients.

Once features are extracted from the images, it is necessary to pre-processing them to make the contribution of each feature equal and the distance in LOF calculation meaningful. We choose the global whitening (principal component transform) as suggested in [18]. By projecting the input data into a new space, the whitening process decorrelates the features and makes them have unit variance in each direction. Because the space projection is based on eigenvalue decomposition of the features' covariance matrix, we discard the components with eigenvalues smaller than 0.01 to make the input data less redundant. The normalization are conducted latter to make the component equally scaled.

3.3 Evaluation Metrics

In this experiment, we use the AUC value (the value of the area under the receiver operating

characteristic curve) to evaluate the performance of our method. The closer the AUC value is to 1, the better the performance of our method is. What's more, the average rank of LOF value can reflect the deviation degree of the test image from the covers. It was taken as an assistant evaluation factor. The images with higher LOF value are more likely to be identified as stego.

4. Experiments Results and Discussion

4.1 Performance of Camera Source Identification

First of all, *K* nearest neighbors of the test image are retrieved simply based on the feature distance. *K* equals 200 in this experiment and the influence of *K* will be discussed in the latter part. In the choice of nearest-neighbor algorithm, apart from the conventional ones, there is kernel nearest-neighbor algorithm [32] derived from support vector machine. By substituting the kernel distance metric for the original one in Hilbert space, it maps the data into a higher dimensional feature space. It is an alternative solution to increase the computational power of classifier. In this experiment, we choose Radial Basis and Sigmoid kernel in comparison with traditional distance metrics Cityblock and Euclidean.

For every camera model, we randomly select 100 images from a single device. A total of 1000 images from 10 different models are used as cover images. Images from the left 32 devices constitute the assisted retrieval database. To investigate the influence of the embedding process to the source camera identification, three different embedding algorithms were conducted on the selected images with four different embedding payloads. The retrieval results are shown in **Table 2**.

Table 2. Camera source identification accuracy in different embedding settings

Embedding algorithms	Embedding rate (bpnc)	Distance measurement			
		Cityblock	Euclidean	Radial Basis	Sigmoid
nsF5	0.05	**0.665**	0.631	0.628	0.621
	0.2	**0.664**	0.630	0.627	0.620
	0.4	**0.662**	0.627	0.624	0.616
	0.6	**0.654**	0.620	0.618	0.608
MB1	0.05	**0.666**	0.631	0.628	0.621
	0.2	**0.665**	0.630	0.627	0.619
	0.4	**0.663**	0.628	0.625	0.615
	0.6	**0.661**	0.626	0.623	0.609
MB2	0.05	**0.664**	0.630	0.627	0.620
	0.2	**0.661**	0.627	0.624	0.615
	0.4	**0.656**	0.622	0.619	0.609
	0.6	**0.655**	0.622	0.619	0.606

From **Table 2**, the retrieval accuracy based on Cityblock has a little advantage over other methods. What's more, there is also a parameter selection problem in kernel nearest-neighbor algorithm [32]. The best results are usually acquired by grid searching. It would increase the uncertainty and computation complexity under unsupervised condition. So we prefer to choose Cityblock as the distance matric in our experiments. On the other hand, the detection rate for cover images is very close to the results of stego images. Therefore, the good news is that there are no great changes of recognition rate between different embedding algorithms and embedding rates. The camera source retrieval features are robust to the changes in embedding, which meets the requirements of steganalysis.

4.2 Performance of the Proposed Framework

For the experiment set, care has been taken to make sure that the test image and the retrieval images come from different camera devices. For every camera model, 100 images are randomly selected from a single device. A total of 1000 cover test images are finally obtained. Similarly, the images from the left devices constitute the assisted retrieval database. Three embedding algorithms are utilized with seven different embedding payloads $p \in \{0.05, 0.1, 0.2...0.6\}$.

For the test image, we retrieval images from the reference database based on camera source identification. The test image and its aided samples form a whole test set. We conduct LOF on the test set to determine the type of the test image. The framework combining image retrieval and LOF is denoted as S-LOF. The comparative detectors are as follows:

(1) M-LOF: we conduct LOF on the test set but that the aided samples are images randomly selected from the reference database;

(2) S-OCSVM: for every test image, we train the OC-SVM classifier on the retrieval images;

(3) M-OCSVM: for every test image, the OC-SVM classifier is trained on randomly selected images;

(4) CSM-SVM: we use traditional supervised binary classification (SVM) method under cover source mismatch scenarios, that is, we trained on one source but test on another with the same embedding parameters.

The number of aided samples and training for OC-SVM is fixed to 200. We repeat the test for 50 times with a different selection of devices. The average value of the 50 tests is used as the final result which is shown in **Table 3**.

Table 3. Comparison of proposed framework with other detectors (AUC value)

Embedding algorithms	Embedding rate (bpnc)	Detection methods				
		S-LOF	M-LOF	S-OCSVM	M-OCSVM	CSM-SVM
nsF5	0.05	0.500	0.498	0.485	0.454	**0.507**
	0.1	0.506	0.498	0.491	0.450	**0.517**
	0.2	0.542	0.494	0.529	0.446	**0.546**
	0.3	**0.616**	0.491	0.603	0.451	0.585
	0.4	**0.707**	0.497	0.685	0.455	0.626
	0.5	**0.798**	0.508	0.755	0.469	0.672
	0.6	**0.869**	0.536	0.807	0.499	0.719
MB1	0.05	0.515	0.496	0.500	0.473	**0.537**
	0.1	0.566	0.493	0.554	0.479	**0.586**
	0.2	**0.700**	0.523	0.677	0.501	0.685
	0.3	**0.801**	0.559	0.759	0.548	0.756
	0.4	**0.871**	0.610	0.809	0.601	0.807
	0.5	**0.915**	0.666	0.835	0.646	0.842
	0.6	**0.941**	0.716	0.847	0.693	0.870
MB2	0.05	0.535	0.492	0.523	0.445	**0.556**
	0.1	**0.632**	0.512	0.619	0.455	0.624
	0.2	**0.803**	0.565	0.760	0.509	0.737
	0.3	**0.894**	0.637	0.823	0.585	0.817
	0.4	**0.942**	0.711	0.845	0.655	0.862
	0.5	**0.962**	0.772	0.852	0.703	0.889
	0.6	**0.974**	0.813	0.854	0.736	0.905

Even though the recognition rate of the camera source identification is far from satisfactory, both methods have a great performance improvement after the image retrieval process. The method proposed in this study performs best among all the methods. This result verifies that the similarity image retrieval based on image statistical characteristics can mitigate the effect of the difference in cover sources. The proposed framework can achieve a universal blind detection when we have no information about the cover source and embedding schemes. However, all of the methods can't overcome the weakness of poor detection performances when the embedding payload is lower than 0.2bpnc, which are almost random guessing.

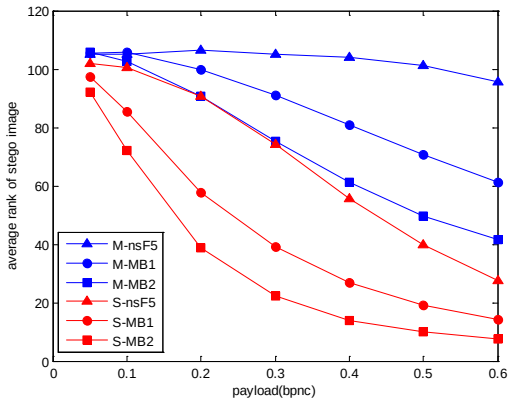

Fig. 2. Average rank of stego image in M-LOF and S-LOF in different embedding settings

As an assist evaluation factor, the average rank of the stego image's LOF value can reflect the performance of the proposed framework from an another aspect. **Fig. 2** shows S-LOF have a much lower average rank of stego image by contrast with M-LOF. It means the test image is more likely to be identified as an outlier in the proposed framework.

4.3 Influence of the Number of Aided Samples

From the result shown in Section 4.1, the detection accuracy of the camera model identification is slightly affected by the embedding rate. We just test one embedding rate to investigate the influence of the aided image number to the detection results. The number of aided samples are ranging from 50 to 400 at intervals of 50. Three different embedding algorithms are conducted at the embedding rate of 0.3bpnc. The detection result of camera source identification and AUC value of our proposed method are shown in **Fig. 3** and **Fig. 4**. The detector exhibits a similar performance trend in other embedding payloads.

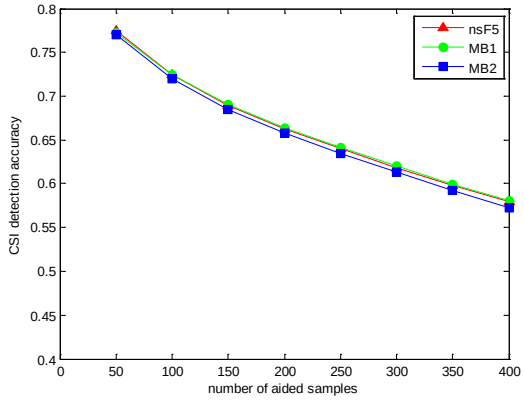

Fig. 3. The detection result of CSI against the number of aided samples

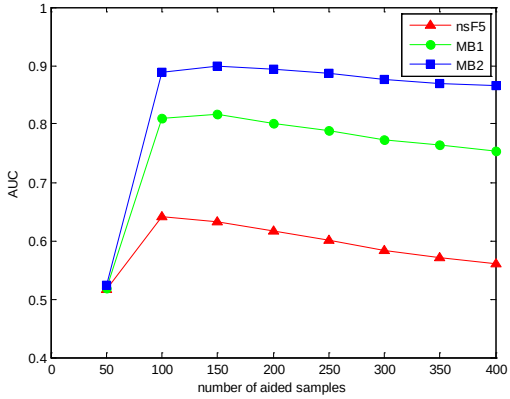

Fig. 4. The AUC value of S-LOF against the number of aided samples

Generally, the shorter distance between two images, the more likely that they are from the same source. This conforms with the result in **Fig. 3** that the retrieval accuracy is almost in a linear decrease with the increasing aided samples. But the performance of our method improved sharply first and decline slightly with the maximum value occurs around 150. The defult value of K = 200, which was used in this study, seems to be a good compromise. This phenomenon can be explained by the reason that the property of stego image does not stand out in insufficient aided samples, whereas too many aided samples may lead to more diversities thus smoothing out the outlier level of the stego image. As the performance just decline slightly when the aided number exceeds 100, we still have many secure options in the aided number selection.

4.4 Computation Complexity

The mean time consumption of four methods detecting single image are compared in **Table 4**. M-LOF consumes the least time for the lack of retrieval and training procedure. S-OCSVM needs to train a specific classifier for each test image, so its detection efficiency is the lowest. Consequently, the proposed framework is of great practical value for its good detection performance and relatively high efficiency.

Table 4. Average time consumption of single image detection (s)

Detection method	S-LOF	M-LOF	S-OCSVM	M-OCSVM
Time consumption	0.047	0.0166	0.0563	0.0279

4.5 Discussion on Modern Steganography and Steganalysis Methods.

We have tested the proposed framework on rich model features and the adaptive steganography algorithms J-UNIWARD [34] and UED [35]. Several steganalysis features were tried and the results shown in **Table 5** are based on the so-called DCTR features [36]. SR-LOF and SR-OCSVM denote the detector LOF and OC-SVM combined with image retrieval and DCTR features. The embedding payload is 0.6 bpnc.

Table 5. Detection results of modern steganography and steganalysis methods.

Embedding algorithms	Detection methods			
	S-LOF	SR-LOF	S-OCSVM	SR-OCSVM
nsF5	**0.869**	0.541	0.807	0.499
MB1	**0.941**	0.536	0.847	0.494
MB2	**0.974**	0.555	0.854	0.507
J-UNIWARD	**0.557**	0.507	0.546	0.494
UED	**0.607**	0.525	0.591	0.507

From the results of SR-LOF and SR-OCSVM in **Table 5**, the detection performance based on rich models is rather frustrating. It seems that the distance measurement fail easily in high-dimensional space. Besides, the feature extraction is more time consuming. The results for embedding algorithm J-UNIWARD and UED are almost random guessing. It is really normal because this algorithm is still hardly detectable in supervised learning. In fact, both of these two problems have not been addressed in the prior works [17][18] by Ker, which just used low-dimensional features and the steganography accessible to the non-expert. Much work remained to be done to extend our framework to the state-of-the-art steganography and steganalysis methods.

5. Conclusion

This study proposes a new blind detection framework combing similarity image retrieval and outlier detection. The experiment results show that the detection performance of the proposed framework is better than the traditional single-class classifier. Additionally, it removes the need for training and avoids the effect of cover source mismatch. The proposed framework does not specialize to any particular embedding algorithm thus achieving universal blind detection. The existing and new blind steganalysis features can be applied to the proposed framework. It has a great prospect for practical application.

There are several directions worth to be explored in future work. In this study, we choose a public database rather than images downloaded from the internet in order to investigate the performance of source camera identification. In the most popular picture-sharing website Flickr, there are millions of images tagged with hundreds of camera models. The images are of diversity size, quality and content which are perfect for our camera source identification. It is necessary to move our work to the real image database with more camera models and image quantities. On the other hand, new image statistical features that are more sensitive to image statistical characteristics but insensitive to embedded changes should be studied. In this study, we briefly tested our method on rich model features and adaptive steganography algorithm, where it seems work less well. So another direction might be to use the modern rich features and multiple anomaly detectors instead of a single LOF to improve the detection accuracy of steganalysis.

Acknowledgement

The authors would like to thank the anonymous reviewers for their helpful comments. Gratitude is also extend to T. Gloe and R. Böhme to build and maintain the Dresden image database. This work was supported by the National Natural Science Foundation of China (Nos. 61572518 and 61272490).

References

[1] 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. Article (CrossRef Link).

[2] V. Holub and J. Fridrich, "Random projections of residuals for digital image steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1996−2006, Dec. 2013. Article (CrossRef Link).

[3] P. Bas, T. Filler, and T. Pevný, "Break our steganographic system: The ins and outs of organizing BOSS," in *Proc. of 13th Information Hiding conference*, pp. 59-70, 2011. Article (CrossRef Link).

[4] I. Lubenko and A. D. Ker, "Steganalysis with mismatched covers: Do simple classifiers help," in *Proc. of 13th Workshop, Multimedia Security*, pp. 11–18, 2012. Article (CrossRef Link).

[5] M. Barni, G. Cancelli, and A. Esposito, "Forensics aided steganalysis of heterogeneous images," in *Proc. of IEEE Int. Conf. Acoustic Speech and Signal Processing*, pp. 1690-1693, 2010. Article (CrossRef Link).

[6] S. Lyu and H. Farid, "Steganalysis using color wavelet statistics and one-class vector support machines," in *Proc. of SPIE, Security, Steganography, Watermarking of Multimedia Contents VI*, vol. 5306, Jun. 2004. Article (CrossRef Link).

[7] T. Pevný and J. Fridrich, "Novelty detection in blind steganalysis," in *Proc. of 10th Workshop, Multimedia Security*, pp. 167−176, 2008. Article (CrossRef Link).

[8] I. Lubenko and A. D. Ker, "Going from small to large data in steganalysis," in *Proc. of IS&T/SPIE Electron. Image*, vol. 8303, p. 83030M, Feb. 2012. Article (CrossRef Link).

[9] G. Cancelli, G. Doerr, I. Cox, and M. Barni, "A comparative study of ±1 steganalyzers," in *Proc. of IEEE Int. Workshop, Multimedia Signal Processing*, pp. 791-796, 2008. Article (CrossRef Link).

[10] T. Pevný and J. Fridrich, "Multiclass detector of current steganographic methods for JPEG format," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 635-650, Dec. 2008. Article (CrossRef Link).

[11] X. Hou, T. Zhang, and G. Xiong et al., "Forensics aided steganalysis of heterogeneous bitmap images with different compression history," *Ksii Transactions on Internet & Information Systems*, vol. 6, no. 8, pp. 1926−1945, Aug. 2012. Article (CrossRef Link).

[12] X. Hou, T. Zhang, and G. Xiong et al., "A novel steganalysis framework of heterogeneous images based on GMM clustering," *Signal Process: Image Communication*, vol. 29, no. 3, pp. 385-399, Mar. 2014. Article (CrossRef Link).

[13] S. Cho, M. Gawecki, and C. Kuo, "Content-dependent feature selection for block-based image steganalysis," in *Proc. of IEEE Int. Symposium on Circuits and Systems*, pp. 1416−1419, 2012. Article (CrossRef Link).

[14] S. Cho, B. Cha, and M. Gawecki et al., "Block-based image steganalysis: Algorithm and performance evaluation," *Journal of Visual Communication & Image Representation*, vol. 24, no. 7, pp. 846−856, Oct. 2013. Article (CrossRef Link).

[15] X. Li, X. Kong, B. Wang, Y. Guo, and X. You, "Generalized transfer component analysis for mismatched JPEG steganalysis," in *Proc. of IEEE Int. Conf. Image Processing*, pp. 4432-4436, 2013. Article (CrossRef Link).

[16] A. D. Ker and T. Pevný, "A new paradigm for steganalysis via clustering," in *Proc. of SPIE - The International Society for Optical Engineering*, vol.7880, Feb. 2011. Article (CrossRef Link).

[17] A. D. Ker and T. Pevný, "Identifying a steganographer in realistic and heterogeneous data sets," in *Proc. of IS&T/SPIE Electronic Imaging. International Society for Optics and Photonics*, vol. 8303, pp. N01–N13, May 2012. Article (CrossRef Link).
[18] A. D. Ker and T. Pevný, "The steganographer is the outlier: Realistic large-scale steganalysis," *IEEE Trans. Inf. Forensics Security*, vol. 9, no.9, pp. 1424−1435, Sep. 2014. Article (CrossRef Link).
[19] W. Ng, Z. He, D. Yeung, and P. Chan, "Steganalysis classifier training via minimizing sensitivity for different imaging sources," *Inform. Science*, vol. 281, pp. 211-224, May. 2014. Article (CrossRef Link).
[20] J. Kodovský, V. Sedighi and J. Fridrich, "Study of cover source mismatch in steganalysis and ways to mitigate its impact," in *Proc. of SPIE, Media Watermark., Security, and Forensics*, vol. 9028, p. 90280J, Feb. 2014. Article (CrossRef Link).
[21] T. Pevný and A. D. Ker, "A mishmash of methods for mitigating the model mismatch mess," in *Proc. of SPIE, Media Watermark., Security, and Forensics*, vol. 9028, p. 90280I, Feb. 2014. Article (CrossRef Link).
[22] Kharrazi, M., H. T. Sencar, and N. Memon. "Blind source camera identification," in *Proc. of IEEE Int. Conf. Image Processing*, pp. 709-712, 2004. Article (CrossRef Link).
[23] Filler, T., J. Fridrich, and M. Goljan. "Using sensor pattern noise for camera model identification," in *Proc. of IEEE Int. Conf. Image Processing*, pp. 1296-1299, 2008. Article (CrossRef Link).
[24] J. Lukas, J. Fridrich, and M. Goljan. "Determining digital image origin using sensor imperfections," in *Proc. of SPIE, Image and Video Communications and Processing*, vol. 5685, pp. 249-260, 2005. Article (CrossRef Link).
[25] M. Goljan, Miroslav, J. Fridrich, and T. Filler. "Large scale test of sensor fingerprint camera identification," in *Proc. of SPIE, Media Forensics and Security*, vol. 7254, 2008. Article (CrossRef Link).
[26] S. Gao, G. S. Xu, and R. M. Hu, "Camera model identification based on the characteristic of CFA and interpolation," in *Proc. of International Conference on Digital-Forensics and Watermarking*, vol. 7128, pp. 268-280. 2011. Article (CrossRef Link).
[27] Magiera, P., Löndahl, C.: ROF Denoising Algorithm (released 2008), http://www.mathworks.com/matlabcentral/fileexchange/22410-rof-denoising-algorithm/content/ROFdenoise.m.
[28] Janssens, Jeroen H. M., I. Flesch, and E. O. Postma. "Outlier Detection with One-Class Classifiers from ML and KDD." in *Proc. of International Conference on Machine Learning and Applications*, pp. 147-153, 2009. Article (CrossRef Link).
[29] M. M. Breunig, H. P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in *Proc. of ACM SIGMOD Int. Conf. Manage. Data*, pp. 93–104, 2000. Article (CrossRef Link).
[30] T. Gloe and R. Böhme, "The 'Dresden Image Database' for benchmarking digital image forensics," in *Proc. of SAC*, pp. 1584-1590. 2010. Article (CrossRef Link).
[31] T. Pevný and J. Fridrich, "Merging Markov and DCT features for multi-class JPEG teganalysis," in *Proc. of SPIE, Media Watermark., Security, Forensics IX*, vol. 6505, pp. 3-14, Feb. 2007. Article (CrossRef Link).
[32] K Yu, L Ji, X Zhang. "Kernel nearest-neighbor algorithm," *Neural Processing Letters*, pp. 147-156, 20002. Article (CrossRef Link).
[33] S. Gao, "A Hybrid Approach for Camera-Model Detection," *International Journal of Security and Its Applications*, 2015, Vol. 9, no. 8. Article (CrossRef Link).
[34] V. Holub, J. Fridrich and T. Denemark, "Universal distortion function for steganography in an arbitrary domain," *EURASIP Journal on Information Security*, pp. 1-13, 2014. Article (CrossRef Link).
[35] L. Guo, J. Ni, and Y. Q. Shi, "An efficient JPEG steganographic scheme using uniform embedding," *IEEE Transactions on Information Forensics and Security*, vol.9, pp. 169-174, 2012. Article (CrossRef Link).

[36] 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, 2015. Article (CrossRef Link).

Yunda Wu received his BS degree in signal and information processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2014, and is currently pursuing the MS degree at Zhengzhou Information Science and Technology Institute. His research interests include steganalysis, digital image forensics, and image processing.

Tao Zhang received his MS and PhD degree in signal and information processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2000 and 2003, respectively. He is currently a professor with the Department of Information Science, Zhengzhou Information Science and Technology Institute. His research interests include information hiding, image processing, and pattern recognition.

Xiaodan Hou received her MS degree in signal and information processing from Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2013. She is currently pursuing the PhD degree at Zhengzhou Information Science and Technology Institute. Her research interests include steganalysis, digital image forensics, and image processing.

Chen Xu received his BS degree in detection guidance & control technology from Xidian University, Xi'an, China, in 2013, and is currently pursuing the MS degree at Zhengzhou Information Science and Technology Institute. His research interests include steganalysis, digital image forensics, and image processing.