Multi-class Blind Steganalysis Based on Image Run-Length Analysis

Jing Dong, Wei Wang, and Tieniu Tan

National Laboratory of Pattern Recognition, Institute of Automation,
Chinese Academy of Sciences, P.O. Box 2728, Beijing

Abstract. In this paper, we investigate our previously developed run-length based features for multi-class blind image steganalysis. We construct a Support Vector Machine classifier for multi-class recognition for both spatial and frequency domain based steganographic algorithms. We also study hierarchical and non-hierarchical multi-class schemes and compare their performance for steganalysis. Experimental results demonstrate that our approach is able to classify different stego images according to their embedding techniques based on appropriate supervised learning. It is also shown that the hierarchical scheme performs better in our experiments.

Keywords: blind steganalysis, multi-class, image steganalysis, run-length analysis.

1 Introduction

Steganography aims at concealing information communication by means of cover medium transmission. It has been a hot topic in information security and has drawn much attention in recent years. On the other hand, steganalysis, which is the counter-technology of steganography aiming at detecting the very presence of secret message in cover medium, serves the urgent needs of network security to block covert communication with illegal or undesirable information.

Various steganalysis techniques have been proposed for tackling steganographic algorithms. These techniques can be roughly ascribed to two categories. One is called specific steganalysis[1] [2] [3] and the other is named blind steganalysis [4] [5] [6] [7] [8]. Specific steganalysis is targeted at a particular known steganographic algorithm, whereas blind steganalysis can detect the presence of hidden data without knowing its embedding method. Since there are a variety of steganographic methods and it is often difficult to assume the knowledge about which embedding methods have been used in real application, blind steganalysis is gaining more attention from researchers.

Usually, blind steganalyzer only makes a binary decision regarding the presence of the hidden message while specific steganalyzer could provide more information with better reliability and accuracy such as estimating the message length or even retrievaling the message content for a targeted steganographic

A.T.S. Ho et al. (Eds.): IWDW 2009, LNCS 5703, pp. 199–210, 2009.

algorithm. The disadvantage of specific steganalysis is that it can not automatically recognize which embedding algorithm is used and can not cope with new algorithms. On the other hand, blind steganalysis has good generality to detect various embedding algorithms, even an unknown algorithm. In a sense, specific steganalysis and blind steganalysis complement each other under a certain framework, that is, multi-class steganalysis. The goal of multi-class steganalysis is to construct a steganalyzer for images capable of not only discriminating cover and stego images but also recognizing the steganographic algorithms used. One can then use this recognition result and apply a specific steganalyzer for further analysis. Also, the detection accuracy of blind steganalyzer could be verified by multi-class steganalyzer by providing a probability of known and unknown steganographic algorithms. Fig.1 shows such an image steganalysis framework by combining the blind, specific and multi-class steganalysis.

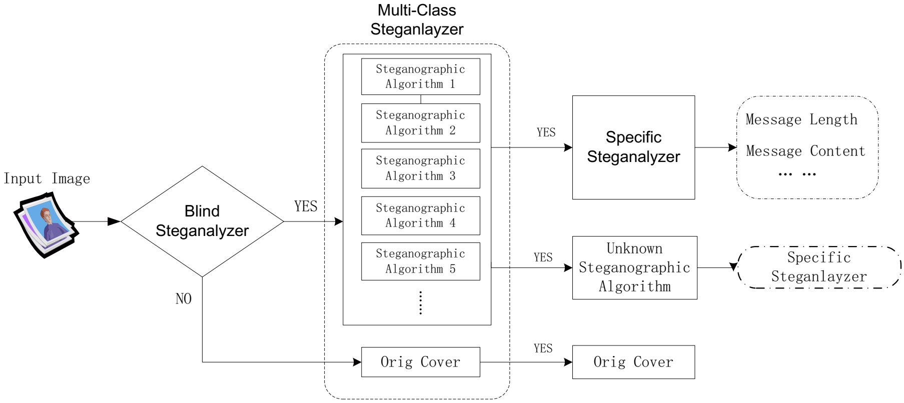

Fig. 1. Framework of hierarchical image steganalysis

The goal of this paper is to investigate multi-class blind image steganalysis according to our proposed run-length based image features [8]. The remainder of this paper is organized as follows. In the next section, we briefly introduce previous work in multi-class steganalysis. Section 3 describes the proposed approach. In Section 4, we carry out some experiments and analyze the performance of both binary detection and multi-class detection results of our proposed scheme. Discussions and conclusions are presented in Section 5.

2 Related Work

There are only a few methods about multi-class steganalysis in the open literature. For JPEG image steganalysis, Pevny and Fridrich [9] used their previously proposed calibrated DCT features for both binary classification and multi-classification for four steganographic techniques (namely F5, OutGuess, MB [10] and JP Hide&Seek). They presented a multi-class steganalyzer using a set of SVM classifiers and studied the parameters for each binary classifier construction. Although there are some misclassifications in their experimental results, their proposed scheme is capable of not only detecting stego images but also classifying them to appropriate stego algorithms at a high embedding rate. In their subsequent work [11], they made a more detailed analysis on multi-classification of JPEG images for their single and double JPEG compression estimation. Also, they combined their DCT-based steganlaysis features with the Markov features proposed by Shi et al.[12] and used these features for multi-classification by a SVM-based multi-classifier. The experimental results showed the detection accuracy of the proposed method is very good although it suffers from an increased false positive rate. Though their study is only focused on JPEG format and also a preliminary study for multi-class steganalysis, they identified several principles for designing the multi-class steganalysis schemes.

Later in the work of [13], Savoldi and Gubian considered a blind multi-class steganalysis system using wavelet statistics. This multi-class system is based on high-order wavelet statistics to recognize four popular frequency domain steganographic algorithms, namely F5 [14], OutGuess[15], JP Hide&Seek [16] and Steghide [17]. In their work, they used soft-margin Support Vector Machine (SVM) with Gaussian kernel and used a 360-D feature vector extracted from image decomposition coefficients based on separable quadrature mirror filters (QMFs). Another work is presented by Wang et al. in [18]. In this paper, they explored two hieratical multi-class steganalysis schemes to recognize popular stego algorithms used for JPEG images and compared the two schemes in terms of accuracy, reliability and computational cost.

The multi-class steganalysis methods mentioned above are all designed for JPEG format and constrained to a few trained popular embedding algorithms. However, since there are many steganographic techniques for BMP images and new embedding algorithms continue to be developed, a more general multi-class steganalysis scheme is highly desirable. This is the main motivation of this paper. In the next section, we will describe our proposed multi-class steganalyzer based on image run-length statistics and a support vector machine.

3 Proposed Approach for Multi-class Steganalysis

There are two key issues in designing a proper multi-class steganalyzer. The first is the extraction of effective features which should be sensitive to various image steganographic techniques. These features should be capable of distinguishing cover and stego images as well as capable of distinguishing different stego techniques. In other words, the ideal distribution of the steganalysis feature space should be something as shown in Fig.2. In this feature space, not only the cover images and stego images can be distinguished, but also the stego images generated by different steganographic schemes form separable clusters. Such image steganalysis features are considered as very effective and powerful for multi-class steganalysis.

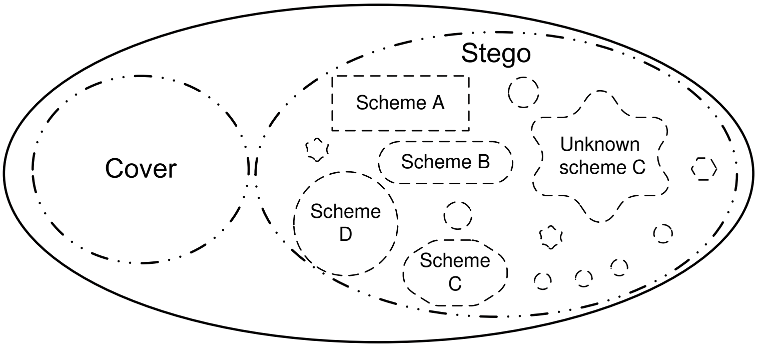

Fig. 2. Illustration of ideal steganalysis feature space

In order to detect different steganographic techniques as much as possible, the proposed feature set should have a good generality. Here, we apply the previously proposed effective run-length based statistic moments as basic features [8]. These features are extracted from image run-length histograms and are very sensitive to data embedding both in spatial domain and in frequency domain.

3.1 Run-Length Based Statistic Moments

Our previously proposed features for steganlaysis in [8] are inspired by the concept of run-length, which was proposed for bitmap-file coding and compression standard in fax transmissions [19]. Normally, a run is defined as a string of consecutive pixels which have the same gray level intensity along a specific linear orientation θ (typically 0°, 45°, 90°, and 135°). The length of the run is defined as the number of repeating pixels in this run. For a given image, a run-length matrix $p(i, j)$ is considered as the number of runs with pixels of gray level i and run length j. For a run-length matrix $p_\theta(i, j)$, let M be the number of gray levels and N be the maximum run length. We can define the image run-length histogram (RLH) as a vector:

$$H_\theta(j) = \sum_{i=1}^{M} p_\theta(i, j), \qquad 1 < j < N \tag{1}$$

This vector represents the sum distribution of the number of runs with run length j in the corresponding image. In order to reduce the effect of different image sizes, the RLH may be normalized by the maximal value of the histogram. Short runs (with smaller j) refer to those runs with a small number of pixels, while long runs (with larger j) imply those runs with a large number of pixels.

For most steganographic algorithms, once a bit of message is embedded in the cover image, one or several corresponding image pixel would be changed slightly to “hide” data, regardless the change is directly caused in spatial domain or reflected by frequency domain, since the data hidden in DCT domain also cause changes of image intensity in the spatial domain. Such attributes of data embedding process would directly affect the local intensity variations of the image. As the image intensity has been changed, the original distribution of image run-length would be altered. That is to say, the original consecutive pixels with identical gray level in a run may turn to different shorter runs. More specifically, the tendency of long runs turning into shorter runs could be due to data embedding. Based on this observation, we proposed a 36-D feature vector for image steganalysis in [8]. Here in this paper, we also take a similar feature set which is slightly modified and improved from the previous feature set. Instead of calculating the Characteristic Function of image run-length histograms, we directly extracted the higher order moments of image run-length histograms according to the following function as our features for multi-class steganalysis. $H(\theta, i)$ represents different run-length histograms along direction θ. More details about the feature extraction may be found in [8].

$$M_n = \sum_{j=1}^{L/2} j^n |H_{(\theta,i)}(j)| / \sum_{j=1}^{L/2} |H_{(\theta,i)}(j)|. \quad 1 < j < N, \quad i = 1, 2, 3; \tag{2}$$

The run-length based feature set has shown very effective performance for blind image steganlaysis not only for detection accuracy but also for computational complexity [8]. Besides, these features are also considered as sensitive features for blind image steganalysis of BMP images as well as JPEG format. Although these features are extracted from spatial domain, they represent the changes in inter-pixel correlation which either steganographic process would cause. Hence we also apply these features for the following multi-class steganalysis schemes. It should be pointed out that the focus of this paper is on the study of the feasibility of run-length analysis for multi-class steganalysis, not on the design of new features per se.

3.2 Multi-class Detector

Another key issue for multi-class steganalysis is the design of proper classifiers. SVM (Support Vector Machine) [20] is a useful technique that provides state-of-the-art performance in a wide variety of application domains. The goal of SVM is to produce a model which could predict class labels of data instances in the testing set which is given only the sensitive features. It performs pattern recognition for two-class problems by determining the separating hyperplane that has maximum distance to the closest points of the training samples. The key issues for SVM is to decide which kernel function is to be used (such as linear, polynomial, radial basis function (RBF), sigmoid etc.) and find the best parameters to construct the training model. Since SVM has shown its optimal and efficient classification performance for large scale learning, it was considered as a popular choice for steganalysis classifiers [4] [12] [21] [22]. For its powerful classification performance and its popularity in use of pattern recognition, we also consider our multi-class detector based on SVM. In this paper the SVM method used is Lib-SVM with a RBF kernel [20].

SVM was originally designed for binary classification. How to effectively extend it for multi-class classification is still under research. There are two ways for multi-class classification. One is a hierarchical multi-classifier which can be realized by constructing and combining several binary classifiers. The other is to consider all data in one optimization formulation and perform multi-classification by one classifier (for example, by regression methods). The formulation to solve multi-class SVM problems depends on the number of classes and is very sensitive to the training data, especially sensitive to outliers. In general it is computationally more expensive to solve a multi-class problem than a binary problem with the same number of data. A comparison between several SVM based multi-classification schemes are described in [23]. Generally speaking, there are three strategies called one-against-all, one-against-one, and directed acyclic graph SVM (DAGSVM) which are designed for solving several binary classification problems for multi-classification. However, for limited data sets, it is believed and suggested in [23] that the one-against-one method is more suitable for practical use than the other methods for multi-classification based on binary classifiers. In this method, training is accomplished by comparing one class against each of the other classes. The goal is to train the multi-class rule based on the majority voting strategy.

As a preliminary study for multi-class steganalysis, we test our proposed run-length based statistics using the "one-against-one" strategy under the following two slightly different schemes.

- Scheme One (S1):We construct the multi-class SVM to classify cover images from different stego images at one time. In this scheme, we simply apply the SVM based multi-classifier to categorize cover images as well as stego images generated by n different embedding algorithms. The number of binary classifiers we used in this scheme is $n(n+1)/2$ (n is the number of known categories of steganographic techniques).
- Scheme Two (S2): In this scheme, we firstly apply a binary SVM as for blind steganalysis to classify cover and stego images. Then we construct a multi-class SVM to classify stego images generated by different known steganographic algorithms. As the primary objective for image steganalysis is to detect whether there are data hidden in cover images, detecting the stego image from clean cover image is the top priority in designing the classifier. Hence, we use a binary SVM classifier for all samples to classify cover and stego images at the first step. Afterwards, we apply a multi-classifier for all labeled stego samples by using a trained multi-classification model to classify images generated by known steganographic algorithms.The number of binary classifiers we used in this scheme is $n(n-1)/2+1$ (n is the number of known categories of of steganographic techniques).

The above two schemes can be considered as one scheme if the feature space of cover and different categories of stego images are well separated from each other. By comparing S1 with S2, the only difference is the number of classes. Since we believe that the distance between cover images and all stego images in the feature space should be larger than the distance among stego algorithms in the feature space (as shown in Figure 2), the optimization problem for SVM to get the best classification curve would be more efficient in S2 than in S1 as the number of classes in S2 is smaller hence the number of binary classifiers used in S2 is fewer. We will investigate this issue in the following experiments in details.

4 Experimental Results

4.1 Database Description

For our experiments, we use the 1338 images downloaded from the Uncompressed Color Image Database (UCID) constructed by Schaefer and Stich [24], available at [25]. All the images in UCID are high resolution uncompressed digital TIFF files with size of 512×384 or 384×512. This database contains various images captured from indoor and outdoor, daylight and night, event and natural scenes, and provides a real and challenging environment for a steganalysis problem. All images were then converted to gray level BMP or JPEG at 75% quality for our experiments. Then, we generated five sets of stego images using the following embedding algorithms. In order to test the effectiveness of our proposed scheme, we only embedded a small amount of messages in our experiments. The embedding rate is below 0.3bpp for BMP images and around 25% message for JPEG image embedding.

#1: Generic LSB embedding method at 0.3bpp;
#2: Non-blind spread spectrum (SS)method [26] at 0.15bpp;
#3: F5 method [14] at 0.25bpnc;
#4: Model Based steganographic method [10] at 0.25bpnc;
#5: Yet Another Steganographic Scheme (YASS) embedding method [27] at 0.15bpnc.

We totally get 6 classes (including cover images) for multi-classification in our experiments. The total number of images we used in our experiments is $1338 \times 6 = 8028$. For each experiment, we divided the images into training and testing sets. There is no overlap between training and testing sets for each experiment. The feature set used in all experiments is obtained from image gray level run-length histograms as mentioned in Section 3.1.

4.2 Detection Performance

Experiments for 2-class Steganalysis. In this experiment, we intend to test the effectiveness of the run-length based features for JPEG image steganalysis as well as for BMP images. We first design some tests for blind steganalysis. Blind means the classifier is able to classify all images into two classes: cover and stego images. The SVM was trained using multiplicative grid search. We compared the detection results for distinguishing the cover images from stego images embedded with each and all specific embedding algorithms in Table 1.

For the first five rows, the training sets and testing sets equally contain 669 cover images and 669 stego images corresponding to the algorithm index. The column of 'Cover'and 'Stego' represents the number of images that were classified as cover or stego under each test. The detection accuracy is calculated by counting the number of images whose cover images are correctly classified as cover and stego images are classified as stego at a 3.5% false positives rate. From this table, we see that the run-length based statistic features are effective to all listed embedding algorithms regardless embedding is performed in the spatial or the frequency domain.

Also, in the last row of this table, which we call 'Cover vs. Mixed' mode, the cover images are the same as in previous tests but the stego images consist of randomly selected 1338 images from all stego image sets (1338 × 5) and are also divided equally into training and testing sets. Hence, in this mode, it is a real blind mode for image steganalysis. We can also see a good detection performance.

Table 1. Blind detection results for trained binary SVM using run-length based features

Embedding Algorithm	Cover	Stego	Accuracy
Cover vs. LSB	608 (90.88%)	641 (95.81%)	93.35%
Cover vs. SS	583 (87.14%)	610 (94.18%)	89.16%
Cover vs. F5	658 (98.36%)	648 (96.86%)	97.61%
Cover vs. MB1	652 (97.46%)	642 (95.96%)	96.71%
Cover vs. YASS	648 (96.86%)	640 (95.67%)	96.26%
Cover vs. Mixed	628 (93.87%)	646 (96.56%)	95.2167%

As shown in Table 1, the run-length based features are able to classify cover images from all stego images generated by either spatial or frequency based embedding algorithms. The trained SVM classifier also serves as a good classifier for universal image steganlysis.

Experiments for Multi-class Steganalysis. Here for multi-class steganalysis, we designed our experiments for two schemes. One was to consider the cover images as one of the classes for multi-classification while the other excluded the cover image as one candidate class since we can perform a blind classification at the first step. The blind detection has already shown a high confidence for cover and stego image classification results in our previous test shown in Table 1. Hence, in order to investigate the multi-class problem among stego images as well as cover and different stego images, here we just design the following two schemes by considering cover as or not as one of the classes for multi-classifier construction.

The training and testing process for multi-classifier is the same for both schemes though the total number of classes is 6 in S1 while 5 in S2 (the cover images are not considered as one class in S2). However, the binary classifier needed for the two schemes are quite different. In S1, we totally need to construct $5(5+1)/2 = 15$ classifiers while in S2 we need $5(5-1)/2+1 = 11$. If we

Table 2. Confusion matrix of the detection accuracy for Scheme One (cover included as one class)

Embedding			Classified as			
Algorithm	Cover	LSB	SS	F5	MB1	YASS
Cover	493(73.7%)	30(4.5%)	126(18.8%)	0(0%)	9(1.3%)	11(1.6%))
LSB	33(4.9%)	609(91%)	20(3%)	0(0%)	6(0.9%)	1(0.1%)
SS	56(8.4%)	6(0.9%)	588(87.9%)	3(0.5%)	13(2%)	3(0.5%)
F5	0(0%)	3(0.5%)	3(0.5%)	571(85.35%)	80(12%)	12(1.8%)
MB1	1(0.1%)	19(2.8%)	126(18.8%)	74(11%)	514(76.8%)	58(8.6%)
YASS	5(0.7%)	2(0.3%)	25(3.7%)	21(3.1%	105(15.7%)	511(76.4%)

Table 3. Confusion matrix of the detection accuracy for Scheme Two (cover excluded as one class)

Embedding		Classified as			
Algorithm	LSB	SS	F5	MB1	YASS
LSB	639(95.5%)	28(4.2%)	2(0.3%)	0(0%)	0(0%)
SS	19(2.8%)	638(95.4%)	14 (2.1%)	8(1.2%)	3(0.5%)
F5	0(0%)	5(0.7%)	586(87.6%)	52(7.8%)	26(3.9%)
MB1	1(0.1%)	23(3.4%)	68 (10.1%)	508(75.9%)	70(10.4%)
YASS	2(0.3%)	24(3.6%)	15(2.2%)	111(16.6%)	517(77.3%)

have more classes for classification, the difference of constructing binary classifier for the two schemes would be larger, which would result in higher complexity for both training and testing.

Table 2 shows the confusion matrix of the detection accuracy for S1 (consider the cover images as one class) and Table 3 presents the confusion matrix of the detection accuracy for S2 (without considering the cover images as one class). Both schemes are based on the SVM multi-classifier with default thresholds and the detection results are obtained at a 3.5% false positive rate. Each class in our experiment contains 669 samples for both training and testing. In S1, we classified totally six classes while in S2 we classified five classes in total. Each row in the tables presents the classification results by counting the number of images being labeled. For example, in Row 2, for the testing sets which consist of 669 stego images generated using the LSB embedding method, there are 33 images classified as cover class and 609 images labeled as LSB class. From Table 2 and Table 3, we can see the two multi-classification schemes based on the SVM classifier achieved good detection performance although there are some misclassifications. Moreover, for S2, the classification accuracy is better than S1 since we excluded the cover images as a class to classifier. We think that the better classification results in S2 may be due to the distribution of steganalysis feature space.

Moreover, we also notice that the multi-classification schemes have a good classification performance on embedding methods for spatial domain as well as frequency domain. Besides, even there are some misclassifications between classes, the misclassification rate between frequency domain methods and spatial domain methods is much lower than that among frequency domain methods or spatial domain methods. That is to say, both of our schemes have a promising detection performance on classifying at least two different categories of stego images (say spatial domain and frequency domain).

5 Conclusion

In this paper, we have investigated a novel multi-class system for image steganlaysis. We have designed two multi-class schemes which are capable of not only detecting stego images but also classifying them into appropriate stego techniques based on the modification of our previously developed features of image run-length statistics. We have constructed a Support Vector Machine (SVM) based multi-classifier to recognize various steganographic algorithms designed for spatial domain as well as for frequency domain. We have also described an evaluation of the generality of the proposed features which are extracted from image run-length histograms for universal image steganalysis. Our feature set shows good distinguishability for JPEG images as well as for BMP images. In order to decrease the computing complexity for multi-classifier construction, we have designed a hierarchical multi-classifier in which the classification of cover and all stego images is performed in advance. Then, the multi-class recognition is done among stego algorithms. Our experimental results have demonstrated that this scheme is more reliable and efficient than the other one which considers the cover and all stego algorithms in one pool for multi-class recognition. Since our approach is able to classify stego images to their embedding techniques under proper supervised learning, we will consider to combine different effective features sets (such as the Markov feature in [12], DCT based feature [22], etc.) for multi-class recognition in order to get more reliable and powerful detection performance in the future.

Acknowledgments. The work presented in this paper was supported by Nature Science Foundation of China (Grant No.60603011).

References

1. Fridrich, J., Goljan, M., Hogea, D., Soukal, D.: Quantitative steganalysis: Estimating secret message length. ACM Multimedia Systems Journal. Special issue on Multimedia Securrity 9(3), 288–302 (2003)
2. Dumitrescu, S., Xiaolin, W., Wang, Z.: Detection of lsb steganography via sample pair analysis. In: Petitcolas, F.A.P. (ed.) IH 2002. LNCS, vol. 2578, pp. 355–374. Springer, Heidelberg (2003)
3. Ker, A.: Resampling and the detection of lsb matching in colour bitmaps. In: Proceedings of SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents VII (2005)

4. Farid, H., Siwei, L.: Detecting hidden messages using higher-order statistics and support vector machines. In: Petitcolas, F.A.P. (ed.) IH 2002. LNCS, vol. 2578, pp. 340–354. Springer, Heidelberg (2003)
5. Fridrich, J., Goljan, M.: Practical steganalysis of digital images — state of the art. In: Security and Watermarking of Multimedia Contents. SPIE, vol. 4675, pp. 1–13 (2002)
6. Harmsen, J.J., Pearlman, W.A.: Steganalysis of additive noise modelable information hiding. In: Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI, pp. 131–142 (2003)
7. Shi, Y.Q., et al.: Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, andneural network. In: ICME 2005, pp. 269–272 (2005)
8. Dong, J., Tan, T.N.: Blind image steganalysis based on run-length histogram analysis. In: 15th International Conference of Image Processing 2008 (ICIP 2008), pp. 2064–2067 (2008)
9. Pevny, T., Fridrich, J.: Towards muti-class steganalyzer for jpeg images. In: Barni, M., Cox, I., Kalker, T., Kim, H.-J. (eds.) IWDW 2005. LNCS, vol. 3710, pp. 39–53. Springer, Heidelberg (2005)
10. Salle, P.: Model based steganography. In: Kalker, T., Cox, I., Ro, Y.M. (eds.) IWDW 2003. LNCS, vol. 2939, pp. 154–167. Springer, Heidelberg (2004)
11. Pevny, T., Fridrich, J.: Determining the stego algorithm for jpeg images. In: Proceddings of Information Security, vol. 153, pp. 77–86 (2006)
12. Shi, Y.Q., Chen, C., Chen, W.: A markov process based approach to effective attacking jpeg steganography. In: Camenisch, J.L., Collberg, C.S., Johnson, N.F., Sallee, P. (eds.) IH 2006. LNCS, vol. 4437, pp. 249–264. Springer, Heidelberg (2006)
13. Savoldi, A., Gubian, P.: A markov process based approach to effective attacking jpeg steganography. In: Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing, vol. 2, pp. 93–96 (2007)
14. Westfeld, A.: High capacity despite better steganalysis(f5). In: Moskowitz, I.S. (ed.) IH 2001. LNCS, vol. 2137, pp. 289–302. Springer, Heidelberg (2001)
15. Provos, N.: Software, `http://www.outguess.org`
16. Latham, A.: Software, `http://linux01.gwdg.de/~alatham/stego.html`
17. Hetzl, S.: Software, `http://steghide.sourceforge.net`
18. Wang, P., Liu, F., Wang, G., Sun, Y., Gong, D.: Multi-class steganalysis for jpeg stego algorithms. In: Proceedings of the 15th International Conference on Image Processing, pp. 2076–2079 (2008)
19. Galloway, M.M.: Texture analysis using gray level run lengths. In: Cornput. Graph. Image Proc., vol. 4, pp. 171–179 (1975)
20. Cortes, C., Vapnik, V.: Support-vector network. In: Proceedings of SPIE Electronic Imageing, Security, Steganography and Watermarking of Nultimedia Contents VII, vol. 20, pp. 273–297 (1995)
21. Kharrazi, M., Sencar, H.T., Memon, N.: Benchmarking steganographic and steganalysis techniques. In: Proceedings of SPIE Electronic Imaging, Security, Steganography and Watermarking of Multimedia Contents VII (2005)
22. Fridrich, J.: Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In: Fridrich, J. (ed.) IH 2004. LNCS, vol. 3200, pp. 67–81. Springer, Heidelberg (2004)

23. Hsu, C., Kin, C.: A comparision of methods for multi-class support vector machines. Technical Report, Department of Computer Science and Information Engineering, National Taiwan University, `http://citeseer.ist.psu.edu/hsu01comparision.html`
24. Schaefer, G., Stich, M.: Ucid - an uncompressed colour image database. In: Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia, pp. 472–480 (2004)
25. Database, U.C.I.: `http://vision.cs.aston.ac.uk/datasets/ucid/ucid.html`
26. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T.: Secure spread spectru, watermarking for multimedia. IEEE Trans.Image Process. 6(12), 1673–1687 (1997)
27. Solanki, K., Sarkar, A., Manjunath, B.S.: YASS: Yet another steganographic scheme that resists blind steganalysis. In: Furon, T., Cayre, F., Doërr, G., Bas, P. (eds.) IH 2007. LNCS, vol. 4567, pp. 16–31. Springer, Heidelberg (2008)