Detecting Information-Hiding in WAV Audios

Qingzhong Liu [1, 2], Andrew H. Sung [1, 2*], Mengyu Qiao[1]
[1]*Computer Science Department and*
[2]*Institute for Complex Additive Systems Analysis*
New Mexico Tech
{liu, sung, qiao}@cs.nmt.edu
**correspondence*

Abstract

In this article, we propose a steganalysis method for detecting the presence of information-hiding behavior in wav audios. We extract the neighboring joint distribution features and the Markov features of the second order derivative, and combine these features with the error response by randomly modifying the least significant bit, then apply learning machines to the features for distinguishing the stego-audios from cover videos. Experimental results show that our method performs well in steganalysis of the audio stegograms that are produced by using Hide4PGP, Invisible Secrets and S-tools4.

1. Introduction

Steganography is the art and science of hiding data in digital images, audios and videos, etc. To the contrary, steganalysis is the art and science of detecting the information-hiding behaviors in these covers. In the past few years, many researchers presented several steganalysis methods to detect the information-hiding behaviors in multiple steganography systems. Most of these methods are focused on the detection of information-hiding in digital images. For example, as one of well-known detectors, Histogram Characteristic Function Center Of Mass (HCFCOM) was once successful in detecting noise-adding steganography [1]. Another well-known method is to construct the high-order moment statistical model in the multi-scale decomposition using wavelet-like transform and then apply learning classifier to the high order feature set [2]. Shi *et al*. [3] proposed a Markov process based approach to detect the information-hiding behaviors in JPEG images. Based on the Markov approach, Liu et al. [4] expanded the Markov features to the inter-bands of the DCT domains and combined the expanded features and the polynomial fitting of the histogram of the DCT coefficients, and successfully improved the steganalysis performance in multiple JPEG images. Other works in image steganalysis can be found in the references [5-10].

In audio steganalysis, Ru *et al*. presented a detection method by measuring the features between the signal and a self-generated reference signal via linear predictive coding [11, 12]; Avcibas designed the content-independent distortion measures as features for classifier design [13]. Ozer *et al*. constructed the detector based on the characteristics of the denoised residuals of the audio file [14]. To detect the information-hiding in audios, Johnson *et al*. set up a statistical model by building a linear basis that captures certain statistical properties of audio signals [15]. Kraetzer and Dittmann proposed a Mel-cepstrum based analysis to perform a detection of embedded hidden messages [16, 17].

In this article, we propose a steganalysis method of Wav audios. Firstly, we extract the neighboring joint distribution features and the Markov features (or neighboring condition distribution features) on the second order derivative of the testing signals. Considering the variation of the statistical characteristics from one signal to another one, we randomly modify the least significant bit of the signal, then compute the joint and condition features on the second derivative of the modified signals. The difference between the features from the original testing and from the modified are calculated. Combining the original features and the difference, we

978-1-4244-2175-6/08/$25.00 ©2008 IEEE

employ learning classifier to discriminate the innocent audio signals and those carrying some hidden data.

2. Feature Extraction

In image processing, second order derivative is widely employed for detecting isolated points, edges, etc. and the methods obtain good performance [18]. We introduce a scheme based on the second order derivative to audio steganalysis. To our knowledge, most audio information-hiding systems modify the bits of the audio signals and change the second order derivative. Here we have the hypothesis, that is, the information-hiding will change the statistical characteristics of the second order derivative. Starting from this point, we explore the detection adventure.

An audio signal is denoted as $f(t)$. Where t is the sample time and $t = 1, 2, ..., N$. The second derivative, denoted by $D_f(\bullet)$, is calculated as follows.

$$D_f(t) = \frac{d^2 f}{dt^2} = f(t+1) + f(t-1) - 2 * f(t) \qquad (1)$$
$$t = 2, 3, ..., N-1.$$

The neighboring joint matrix J_{D_f} and the neighboring condition matrix C_{D_f} are constructed as follows:

$$J_{D_f}(i,j) = \frac{\sum_{t=2}^{N-2} \delta(D_f(t) = i, D_f(t+1) = j)}{N-3} \qquad (2)$$

$$C_{D_f}(i,j) = \frac{\sum_{t=2}^{N-2} \delta(D_f(t) = i, D_f(t+1) = j)}{\sum_{t=2}^{N-2} \delta(D_f(t) = i)} \qquad (3)$$

Considering the variation of the statistical characteristics of audio individuals, to improve the statistical differential expression of the features, we randomly modify the least significant of the testing audio, and the modified signal is denoted as $f'(t)$, $t = 1, 2, ..., N$. According to the formulas (1) to (3), we build the neighboring joint matrix $J_{D_{f'}}$ and the neighboring condition matrix $C_{D_{f'}}$, the differences between J_{D_f} and $J_{D_{f'}}$, C_{D_f} and $C_{D_{f'}}$, are given

$$DJ(i,j) = J_{D_f}(i,j) - J_{D_{f'}}(i,j) \qquad (4)$$

$$DC(i,j) = C_{D_f}(i,j) - C_{D_{f'}}(i,j) \qquad (5)$$

The joint matrix J_{D_f} in (2), the condition matrix C_{D_f} in (3), and the differences in (4) and (5) are the features of which the subset will form the final detector.

3. Feature Selection

In (2)-(5), the values of *i* and *j* are set from -8 to 8, so each matrix consists of 289 elements or features, total 289×4 = 1156 features. Generally, some of features are useless, some are significant for discriminating covers and steganograms. Analysis of Variance (ANOVA) is widely used for picking the features with high significance [19, 8]. However, the interaction of the features can't be embodied in ANOVA. Considering the possible interaction of the four types of features mentioned in feature extraction, we form the final feature set according to the following method.

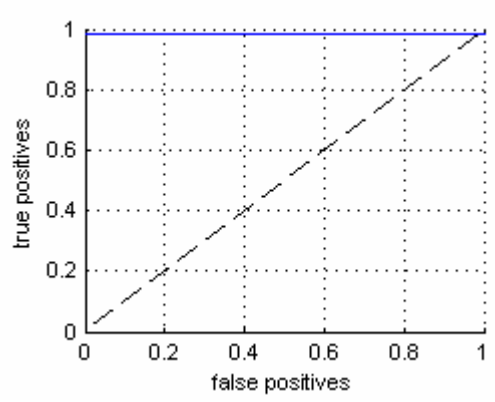
1. If $J_{D_f}(a,b)$ has good statistical significance, then it is put to the final feature set; meanwhile, $C_{D_f}(a,b)$, $DJ(a,b)$, and $DC(a,b)$ are picked up and placed to the final feature set .
2. If $C_{D_f}(a,b)$ has good statistical significance, then it is put to the final feature set; meanwhile, $J_{D_f}(a,b)$, $DJ(a,b)$, and $DC(a,b)$ are picked up and placed to the final feature set .
3. If $DJ(a,b)$ has good statistical significance, then it is put to the final feature set; meanwhile, $C_{D_f}(a,b)$, $J_{D_f}(a,b)$, and $DC(a,b)$ are picked up and placed to the final feature set .
4. If $DC(a,b)$ has good statistical significance, then it is put to the final feature set; meanwhile, $C_{D_f}(a,b)$, $J_{D_f}(a,b)$, and $DJ(a,b)$ are picked up and placed to the final feature set .

4. Experimental Results

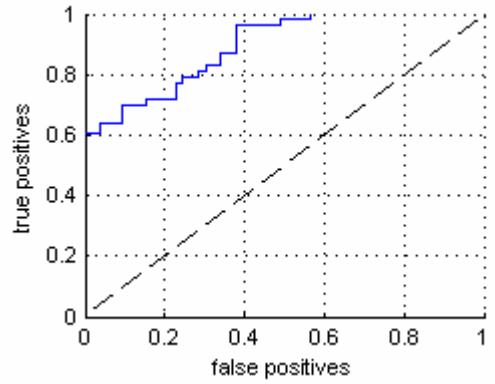
We hid different data in 215 WAV audios and generated three types of audio steganograms by the hiding tools Hide4PGP [20], Invisible Secrets [21], and S-tools 4 [22]. The four types of features are extracted and the final feature sets are determined according to the description in part 3. 75% of the feature sets are employed for constructing the classification model, the other 25% of the feature sets are used for testing. The training sets and testing sets are randomly chosen. We did the experiments 20 times in each detecting. The testing results consists of true positive (TP), true negative (TN), false positive (FP), and false negative (FN). The testing accuracy is calculated by (TP+TN)/(TP+TN+FP+FN). The table 1 lists the testing accuracy values with the use of a Support Vector Machine (SVM) [23].

Table 1. The testing accuracy of the audio steganalysis

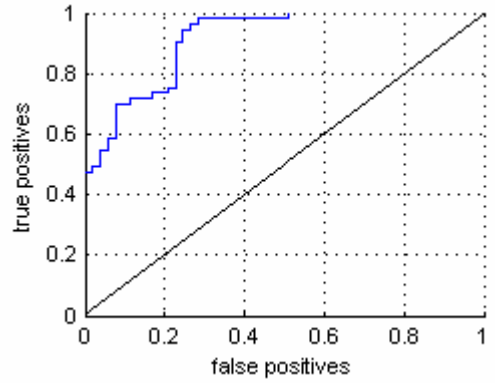
Audio Hiding Tools	Testing accuracy
Hide4PGP	99.1%
Invisible Secrets	76.3%
S-tools 4	72.7%



(a). ROC curve of steganalysis of Hide4PGP



(b). ROC curve of steganalysis of Invisible Secrets



(c). ROC curve of steganalysis of S-tools 4

Figure 1. The steganalysis performance of the audios.

Figure 1 show the ROC curves of the detection performances.

5. Discussion

Experimental results show that our method is good in detecting the information-hiding in the audio steganograpms generated by using Invisible Secrets and S-tools 4 and is very good in detecting the information-hiding in the audio steganograms produced by using Hide4PGP. It clearly indicates that the information-hiding modifies the characteristics of the second order derivative and implies hat the second order derivative is not only good in detecting the isolate points and edges in image processing but also very good in detecting the information-hiding in audios.

The steganalysis performance in detecting Hide4PGP audio steganograms is much better than the detection of the audio steganograms produced by using Invisible secrets and S-tools 4. We analyzed the embedding procedures of these three hiding tools. It shows that, compared to Invisible Secrets and S-tools 4, Hide4PGP has a bigger embedding capacity; in the audio steganograms, the modified bits are not restricted in the least bit, but the last few least significant bits, and hence, it makes more modification to the original signal and results in the more significant change to the second order derivative.

We did not further study the feature selection. By employing some methods of feature selection and choosing an optimal feature set, the steganalysis performance could be improved.

6. Conclusion

In this paper, we first introduce the second order derivative, which is widely used in the isolation and edge detection in image processing, to the steganalysis of audios. We designed the neighboring joint features and Markov features of the second order derivative, and group these features and the difference of the features between the testing signal and the features extracted from the modified version that is generated by randomly modifying the least significant bits. Experimental results show that our method is good in detecting the audio steganograms produced by using Invisible Secrets and s-tools 4 and performs well in steganalysis of Hide4PGP in digital WAV audios.

7. Acknowledgment

The authors gratefully acknowledge the support for this research from ICASA, a division of New Mexico Tech.

References

[1] J. Harmsen and W. Pearlman. Steganalysis of Additive Noise Modelable Information Hiding. *Proc. of SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents,* V. 5020, pp.131-142, 2003.

[2] S. Lyu and H. Farid. How Realistic is Photorealistic, *IEEE Trans. on Signal Processing*, 53(2): 845-850, 2005.

[3] Y. Shi, C. Chen and W. Chen. A Markov process based approach to effective attacking JPEG steganography, *Lecture Notes in Computer Sciences,* vol.437, pp.249-264, 2007.

[4] Q. Liu, A. Sung, B. Ribeiro and R. Ferreira. Steganalysis of Multi-class JPEG Images Based on Expanded Markov Features and Polynomial Fitting. *Proc. International Joint Conference on Neural Networks*, in press.

[5] Q. Liu and A. Sung. Feature Mining and Nuero-Fuzzy Inference System for Steganalysis of LSB Matching Steganography in Grayscale Images. *Proc. of 20th International Joint Conference on Artificial Intelligence,* pp. 2808-2813, 2007.

[6] Q. Liu, A. Sung, J. Xu and B. Ribeiro. Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography, *Proc. of 18th International Conference on Pattern Recognition*, ICPR (1), pp. 1208-1211, 2006.

[7] Q. Liu, A. Sung, Z. Chen and J. Xu. Feature Mining and Pattern Classification for Steganalysis of LSB Matching Steganography in Grayscale Images. *Pattern Recognition,* 41(1): 56-66, 2008.

[8] Q. Liu, A. Sung, B. Ribeiro, M. Wei, Z. Chen and J. Xu. Image Complexity and Feature Mining for Steganalysis of Least Significant Bit Matching Steganography. *Information Sciences,* 178(1): 21-36, 2008.

[9] J. Fridrich. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes. *Lecture Notes in Computer Science,* vol. 3200, Springer-Verlag, pp. 67-81, 2004.

[10] T. Pevny and J. Fridrich. Merging Markov and DCT Features for Multi-Class JPEG Steganalysis. *Proc. SPIE Electronic Imaging, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, 2007.

[11] X. Ru, H. Zhang and X. Huang. Steganalysis of Audio: Attaching the Steghide. *Proc. the Fourth International Conference on Machine Learning and Cybernetics*, pp. 3937-3942, 2005.

[12] X. Ru, Y. Zhang and F. Wu. Audio Steganalysis Based on "Negative Resonance Phenomenon" Caused by Steganographic Tools. *Journal of Zhejiang University SCIENCE A*, 7(4):577-583, 2006.

[13] I. Avcibas. Audio Steganalysis with Content-independent Distortion Measures. *IEEE Signal Processing Letters*, 2006 13(2):92-95.

[14] H. Ozer, B. Sankur, N. Memon and I. Avcibas. Detection of Audio Covert Channels Using Statstical Footprints of Hidden Messages. *Digital Signal Processing*, 16(4):389-401, 2006.

[15] M. Johnson, S. Lyu and H. Farid. Steganalysis of Recorded Speech. *Proc. SPIE*, vol. 5681, pp.664-672, 2005.

[16] C. Kraetzer and J. Dittmann. Pros and Cons of Mel-cepstrum Based Audio Steganalysis Using SVM Classification. *Lecture Notes in Computer Science*, vol. 4567, pp. 359-377, 2008.

[17] C. Kraetzer and J. Dittmann. Mel-cepstrum based steganalysis for voip-steganography. *Proc. SPIE* Vol. 6505, San Jose, CA, USA, 2007. SPIE and IS&T, SPIE.

[18] R.Gonzalez and R. Woods. *Digital Image Processing*. 3rd edition, ISBN: 9780131687288, Prentice Hall, 2008.

[19] T. Hill and P. Lewicki. Statistics: Methods and Applications. ISBN: 1884233597, StatSoft, Inc., 2005.

[20] http://www.heinz-repp.onlinehome.de/Hide4PGP.htm

[21] http://www.invisiblesecrets.com/

[22] http://digitalforensics.champlain.edu/download/s-tools4.zip

[23] V. Vapnik, *Statistical Learning Theory*, John Wiley, 1998.