Front. Electr. Electron. Eng. China 2010, 5(2): 203–206
DOI 10.1007/s11460-010-0010-5

RESEARCH ARTICLE

Min LEI, Yu YANG, Xinxin NIU, Shoushan LUO

Audio steganalysis in DCT domain

Abstract A sort of audio watermarking algorithm in discrete cosine transform (DCT) domain can embed secret information through modification of the distinction between positive and negative direct current (DC) coefficients. Such an algorithm achieves a good balance between robustness and imperceptibility. This paper points out that steganographic methods change statistical characteristics of DC coefficients. It also states that the difference between positive and negative DC coefficients can detect whether an audio has hidden information or not. Experiment results justify that the algorithm accuracy is 79%.

Keywords steganography, steganalysis, audio, discrete cosine transform (DCT)

1 Introduction

Steganography is the art of hiding communication, which uses innocuous-looking documents, such as text, image, audio, video, network protocol, and software, as the cover, uses redundancy of the objects themselves, embeds secrete information into the objects and realizes covert communication. Steganography must be transparent in some level and the process does not markedly modify the perception characteristics of the objects.

With the rapid development of steganography technology and the Internet, ordinary people can now get steganographic tools easily via Internet. However, illicit use of the tools might become a threat to the security of the worldwide information infrastructure. Steganalysis is a technique that can detect objects as either hiding information or not. It not only plays a significant role in information countermeasures, but also can prevent the illicit use of steganography to guarantee the political and public safety of a country, and promotes the continuous development of steganography algorithm.

The research of steganalysis has a high theoretic and practical value. According to its applicable scope, steganalysis can be divided into specific steganalysis and universal steganalysis. Specific steganalysis analyses a particular algorithm and the accuracy is higher. Universal steganalysis is unrelated to the specific one, but its accuracy is lower.

Image steganalysis has made a great progress recently, but audio steganalysis methods are relatively unexplored. Audio steganalysis mainly includes least significant bit (LSB) [1], MP3Stego [2,3], phase information hiding steganalysis [4], and echo hiding steganalysis [5,6].

Recently, some papers regarded steganalysis as a classification problem. That is to say, they considered that the information can be detected by a classifier. The idea of analyzing information by a classifier was first proposed in Ref. [7]. Based on Refs. [6,8], a steganalysis algorithm was proposed which applied to four algorithms, such as LSB and echo hiding steganalysis. At present, steganalysis in discrete cosine transform (DCT) domain can often be done by a classifier. Reference [9] set up the classifier by genetic algorithm, constituted the vectors with features selected by sequential floating search method (SFSM), then steganalyzed DCTwHAS algorithm. Reference [8] steganalyzed DCTwHAS algorithm by support vector machine (SVM) classifier through the algorithm of selecting features.

Reference [10] proposed a kind of audio watermarking algorithm in DCT domain in 2007. It uses the stable characteristics of direct current (DC) coefficient symbol when it is attacked in DCT frequency spectrum and then embeds secret information through modifying the difference between the positive and negative of the DC coefficient. The algorithm achieves good balance between robustness and imperceptibility. On the basis of fully utilizing the principal of steganographic algorithm, this paper points out that the steganographic methods change the statistical characteristics of DC coefficient and proposes a kind of steganalysis method based on the difference between the positive and negative of the DC coefficient.

Received January 20, 2010; accepted February 22, 2010

Min LEI (✉), Yu YANG, Xinxin NIU, Shoushan LUO
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
E-mail: leimin@bupt.edu.cn

Watermarking algorithm and its properties are simply described in Sect. 2. The principle of steganalysis algorithm used in this paper is discussed in Sect. 3. Experimental steps and results of steganalysis are introduced in Sect. 4. Section 5 is the conclusion of this paper.

2 Description of audio watermarking in DCT domains

2.1 Introduction of algorithm

Reference [10] proposed a kind of audio watermarking algorithm in DCT domains, the principle of which is as follows. The two-valued watermarking serial of L bit long which will be embedded is denoted as

$$W(i) = \{1, -1\},\ i = 1,2,...,L.$$

The original audio signal denoted as $x(t)$ is cut into segments. Each segment has N samples. DCT transformation is applied to each frame, and 1 bit watermarking information is embedded per M frames. The relation of L, N, and M is as follows:

$$LM = \frac{\text{length}}{N}. \quad (1)$$

DCT positive and negative transformation of per frame information is essential during the process of watermarking information embedding. The original signals divide LM frames and the length of per frame into N. For the convenience of discussion, we represent the coefficient after DCT transformed per framed information as follows:

$$F(n) = \left\{F_i(n) | i = 1,2,...,\frac{\text{length}}{N}\right\},\ n = 1,2,...,N, \quad (2)$$

where $F(1)$ is DC coefficient and the left are all alternating current (AC) coefficient.

The steps of watermarking algorithm are given as follows.

Step 1 Divide $F(1)$ the set of DC coefficients of all fragments, into L subsets. Each subset is denoted as FDC and the length of per section is M. The kth coefficient of the ith subset is denoted as follows:

$$\text{FDC}_i(k),\ i = 1,2,...,L,\ k = 1,2,...,M. \quad (3)$$

Step 2 Embed watermarking information by adjusting the quantity of positive and negative number in $\text{FDC}_i(k)$. Represent the quantity of positive with $\text{FDC}_i(k)^+$ and the quantity of negative with $\text{FDC}_i(k)^-$, and also D represents the intensity of the embedding.

If $W(i) = 1$, modify the positive and negative of data in $\text{FDC}_i(k)$, which satisfies

$$\text{FDC}_i(k)^- - \text{FDC}_i(k)^+ > D. \quad (4)$$

Otherwise, if $W(i) = -1$, modify the positive and negative of data in $\text{FDC}_i(k)$, which satisfies

$$\text{FDC}_i(k)^+ - \text{FDC}_i(k)^- > D. \quad (5)$$

In order not to influence the quality of audio signals, modify from the minimum of absolute value among $\text{FDC}_i(k)$, mark $\text{FDC}_i(k)^*$ instead of $\text{FDC}_i(k)$ after adjusted.

Step 3 Transform inversely adjusted DCT coefficient, and acquire the watermarking audio signal $x(t^*)$.

2.2 Analysis of algorithm robustness

The experiment of reduce attack of the algorithm in Ref. [10] shows that the algorithm has a good resistance ability when the algorithm was attacked with Echo, Smooth, Amplify, FlippSample, Addsinus, etc. by Audio Stirmark software. The data of the experiment show that the error code rate from all kinds of attacked watermarking is almost 0. For MP3 compression attack, the experiment shows that DC coefficient algorithm is better than the AC coefficient algorithm in resistance of MP3 compression attack. We attacked this watermarking algorithm with additive noise to test the robustness of the algorithm under additive white noise. The experiment shows that when the noise ratio is more than 20 dB, the error code rate is 0. Also, we attack the algorithm with resample and the experiment shows that the error code rate is almost 0 if we modify the resample of transmission frequency. Good robustness of the algorithm was shown in different kinds of experiments.

2.3 Analysis of transparence of algorithm

Reference [10] measured the algorithm transparence by subjective evaluation MOS which is commonly used, the measurement signal of which shows the absolutely same watermarking information when separately embedding the intensive D of 5,10,15,25,35,55,75,95. The data of the experiment show that when D is 25 the mark of MOS is 5. When we use D of 55 in the robustness experiment, the mark of MOS is more than 4.5 which is also the class of high quality. The experiment shows that the watermarking algorithm can guarantee watermark transparence when the robustness is enough. Meanwhile, according to the cover thresholds of psychological acoustics, Ref. [10] proposed a kind of method to measure the quality of watermarking signal sensitivity, the experiment of which shows that the watermarking algorithm has a good transparence.

3 Steganalysis

Based on the analysis of the above steganography, we find that embedding secret information needs to adjust the DC

coefficient in DCT in steganography process, and the steganography algorithm changed the DC coefficient in DCT of the original audio. According DCT transformation is defined as follows:

$$y(1) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} x(n) \cos \frac{\pi(2n-1)(k-1)}{2N}$$

$$= \frac{1}{\sqrt{N}} \sum_{n=1}^{N} x(n), \quad (6)$$

where $x(n)$ denotes the nth sample of spatial signal, $y(1)$ denotes the DC coefficient of DCT transformation, and k denotes the kth frequency component. As we compute DC coefficient, k is valued as 1.

The steganography algorithm changed the mean of sectional signals and made the number of the section, which is the positive and negative values of mean, satisfy some rules. Then the statistical characteristics of DC coefficient symbol in DCT are changed. The regularity of DC coefficient symbol in DCT is improved.

To describe it conveniently, we call the number of positive fragments NPMF for short, the number of negative fragments NNMF, the difference ratio of positive and negative fragments DR and define DR as follows:

$$\mathrm{DR} = \frac{|\mathrm{NPMF} - \mathrm{NNMF}|}{\min(\mathrm{NPMF}, \mathrm{NNMF})}. \quad (7)$$

We proposed a new steganalysis called difference ratio steganalysis, which detects objects as hiding information or not by the difference ratio. According to the principle of steganalysis, the number of positive and negative mean fragments after steganography is almost equal, so the DR before steganography is less than the DR after steganography. If we re-steganography all objects to be detected, the closed number of positive and negative mean fragments after the first steganography and the variation scope of positive and negative mean fragments after the re-steganography of steganographic objects is not as obvious as the cover works. Calculate the ratio value of DR before and after steganography, which works is obviously higher than steganographic objects, and judge the detected objects as steganographic one or not through the threshold value.

4 Experiment and analysis of characteristics

The preparations of the experiment are:

1) Prepare 72 audio documents, whose frequency is 8000 Hz, including the dialogs of males and females.

2) Randomly select 36 documents from the 72 prepared documents.

3) Embed secret information using steganography algorithm in Sect. 2. The length of frame is 256 sample points, and 1 bit secret information is hidden per 10 frames. The steganography intensity D is 5.

Then steganalysis of the 72 documents are detected as follows:

1) Calculate all values of DR of objects to be detected and mark as DR1.

2) Re-steganography all objects to be detected and the parameters of re-steganography are: 128 sample points is one frame and hide 1 bit information with 5 frames and also the intensity of steganography is 3.

3) Calculate all values of DR of objects after re-steganography and mark as DR2.

4) Get Q = DR1/DR2.

The results of the experiment are shown in Table 1.

Table 1 Q value of 72 documents in steganalysis

cover audio	stego audio	cover audio	stego audio	cover audio	stego audio
18.81	3.49	10.03	15.58	25.00	21.76
29.64	8.91	159.81	6.26	41.65	14.97
1111.92	5.33	27.05	4.21	16.21	11.99
39.90	11.75	17.20	197.54	26.03	6.44
38.65	5.08	22.28	12.29	16.12	24.01
33.99	46.46	17.78	10.96	19.44	8.54
21.97	5.77	21.61	3.29	12.91	2.33
21.08	4.89	20.49	5.90	5.62	1.65
51.79	17.31	7.58	2.92	3.00	1.99
45.17	13.54	24.50	5.22	1.97	0.57
12.44	21.80	22.14	0.39	0.36	1.63
29.31	8.16	16.78	0.77	18.66	10.39

According to the algorithm principle of difference ratio steganalysis, the number of positive and negative means that fragments after steganography is almost equal and the quality of positive and negative means that fragments after the first steganography is much closed. The variation scope of positive and negative means that fragments after re-steganography of stego work is not as obvious as cover works presents. Therefore, Q of cover works is much bigger than Q of stego work. When $Q \leqslant T$, $t = 15$ is the threshold and the object is a steganography one. While when $Q > T$, the object is a natural one. To analyze the result conveniently, represent too big Q value with 30. The experimental analysis results are shown in Fig. 1.

Characteristics of steganalysis are mainly judged through evaluating of accuracy, false alarm rate, and missed detection rate of steganalysis. False alarm rate is the probability of deciding that a cover work is a stego work. Missed detection rate is the probability of deciding that a stego work is a cover. From the analysis result in Fig. 1, we can see that among 72 works the number of wrongly decided works is 15, so the accuracy is 57/72 = 79.17%. Among the number of stego work $Q > T$ which were falsely decided to cover works is 7, missed detection rate is 7/72 = 9.72%. The number of cover works $Q \leqslant T$ which

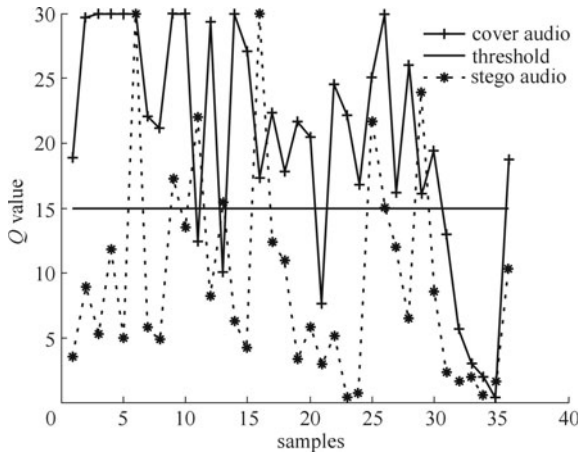

Fig. 1 Analysis of experimental results

were wrongly decided to steganography is 8 and false alarm rate is 8/72 = 11.11%.

5 Conclusion

Reference [10] proposed a kind of audio watermarking algorithm that achieves a good balance between robustness and imperceptibility, and the amount of information steganography of the watermarking algorithm is comparably small, so the steganalysis is very difficult. We find that the statistical characteristics of DC coefficient symbol in DCT are changed during the process of steganography through analysis. After steganography, the regularity of DC coefficient symbol in DCT is improved. Therefore, we proposed a kind of algorithm of difference ratio steganalysis. The accuracy of detection of this steganography algorithm is very high no matter whether detection fragments are the same with steganography fragments or not.

Acknowledgements This work was supported by the National Basic Research Program of China (No. 2007CB311203), the National Natural Science Foundation of China (Grant No. 60821001), the 111 Project (No. B08004), and the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20070013007).

References

1. Zeng W, Ai H J, Hu R M, Liu B, Gao S. Steganalysis of LSB embedding in audio signals based on sample pair analysis. In: Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing. 2007, 2960–2963
2. Song H, Xin Q L, Li W Q, Dai Y Q. MP3Stego hiding and detecting research. Acta Scientiarum Naturalium Universitatis Sunyatseni, 2004, 43(z2): 221–224 (in Chinese)
3. Wang S Z, Zhang X P, Zhang K W. Steganography and Steganalysis. Beijing: Tsinghua University Press, 2005, 143–145
4. Zeng W, Ai H J, Hu R M. A novel steganalysis algorithm of phase coding in audio signal. In: Proceedings of the Sixth International Conference on Advanced Language Processing and Web Information Technology. 2007, 261–264
5. Yang Y, Lei M, Niu X X, Yang Y X. VDSC steganalysis algorithm of echo hiding. Journal on Communications, 2009, 30(2): 83–88 (in Chinese)
6. Ozer H, Avcibas I, Sankur B, Memon N D. Steganalysis of audio based on audio quality metrics. Proceedings of SPIE, 2003, 5020: 55–66
7. Johnson M K, Lyu S, Farid H. Steganalysis of recorded speech. Proceedings of SPIE, 2005, 5681: 664–672
8. Ozer H, Sankur B, Memon N D, Avcibas I. Detection of audio covert channels using statistical footprints of hidden messages. Digital Signal Processing, 2006, 16(4): 389–401
9. Bao C L, Huang Y F, Zhu C Y. Steganalysis of Compressed Speech. In: Proceedings of IMACS Multiconference on Computational Engineering in Systems Applications. 2006, 1: 5–10
10. Wen Q, Wang S X, Nian G J. Audio watermarking in DCT domain: algorithm and measurement of imperceptibility. Acta Electronica Sinica, 2007, 35(9): 1702–1705 (in Chinese)