Active Steganalysis of MP3Stego

Yawai Tint, Khin Than Mya
University of Computer Studies, Yangon
yawai.ywt@gmail.com,khinthanmya@gmail.com

Abstract

The goal of steganalysis is to detect and/or estimate potentially hidden information from observed data. Steganalysis not only plays a significant role in information countermeasures, but also can prevent the illicit use of steganography. This paper develops an active steganalysis system for detecting hidden messages, by estimating frames with hidden message and message length in compressed audio files produced by MP3Stego. Principle Component Analysis (PCA) is applied not only to estimate uncorrelated components but also help to detect whether the received MP3 streams are steganography or original. In this steganalysis system, hidden messages can be detected in the PCA (whitening) stage. Independent Component Analysis (ICA) attempts to separate a set of steganographic signals from original signals. By analyzing the nature of MP3 signals (frame header, side information), frame with secret message can be detected. The results of empirical tests reach 97% and conclude that detection accuracy of the proposed steganalysis system is convenient for MP3Stego embedded contents. Experiments shows that the proposed method can be used quite effectively to detect locations of messages embedded using nature of MP3 signal.

Keywords*: Steganalysis, MP3, Principle Component Analysis (PCA), Independent Component Analysis (ICA), Part2_3_length, Global_gain*

1. Introduction

A new secret communication technology, steganography is to enable convert communication by hiding data in digital covers such as images, audios and videos, etc [1]. Various steganography methods and software have been widely applied. Correspondingly, steganalysis techniques are developed to detect the existence of hidden information. Steganalysis is the opposite of steganography, and aims at detecting and analyzing the hidden information in digital media. Steganalysis is the scientific technology to decide if a medium carriers some hidden messages or not and if possible, to determine the hidden messages in cover objects.

Audio is an important communication way for people, and therefore is a convenient medium secure communications. Audio steganography is a useful means for transmitting convert battlefield information via and innocuous cover audio signal. MP3 audio are prevalently exchanged and widely used, which causes less suspicious than other audio formats.Secret messages are embedded into MP3 audio, it will be difficult to distinguish whether the perceptual distortion is caused by steganography or MP3 compression.

Due to the suitability of MP3 audio as steganographic cover [2], several stego tools for MP3 audio have been arisen such as MP3Stego [3], UnderMP3Cover [4], Stego-Lame [5]. Among them, MP3Stego is a most typical one. It can achieve so good imperceptibility that it is hard to distinguish between background noise and steganographic distortion when the original audio is unavailable.

In this paper, that can detect the existence of hidden messages, and separate signal from mixture source. In addition, estimates frame with hidden message and message length. Although multiple steganalysis methods were designed for detecting information hiding in uncompressed audios in the past years, the information hiding behavior in compressed audios, such as MP3 audios, has been barely explored due to the complication and the variety of the compression methods. This paper focuses on MP3 files. In order to discriminate stego audios from clear normal ones, that embed random data into a (possibly) stego file by using MP3Stego.

To present the basic principle of this new steganalysis technique based on ICA, this paper is restricted to steganalysis with the simplest ICA model. The objective of this paper is to introduce an efficient ICA based steganography detection and extraction scheme for audio steganography. A robust batch ICA algorithm is applied in the steganography detection. By analyzing the nature of MP3 signal to estimate frame with hidden message. The simulation results and performance are shown for various types of signal.

2. Related Work

In audio steganalysis, Qingzhong Liu presented a novel stream data mining for audio steganalysis, based on second order derivative of audio streams. That extracted Mel-cepstrum coefficients and Markov transition features on the second order derivative; a support vector machine was applied to the features

for discovery of the existence of covert message in digital audios [7].

Y.Huang analyzed the properties of the audio information hiding tool by MP3Stego and calculated the statistics of part23 length and stuffingBits in mp3 files. That estimated the size of embedded text accurately by calculating the variance sequence of the block length [12]. Q. Ding [13] approached to Steganalysis of Analysis-by-synthesis Compressed Speech. A steganalysis method for analysis-by-synthesis (AbS) compressed speech is proposed. In this steganalysis method, the probability difference of 0 and 1 and five statistics, including sum of histogram local flatness, sum of histogram local extremum difference, sum of histogram local variance, sum of histogram characteristic function, are used as distinguishing features. SVM classifiers are employed to discriminate stego speech from cover speech.

D.Yan [16] presented a detection method for MP3Stego based on the differential statistics of quantization step. He found that the quantization step which is an important parameter of MP3 encoding is affected during embedding. The standard deviation of the second order differential sequence from quantization step is adopted as the classification feature.

In this article, propose active steganalysis system of MP3 signal. Firstly, decoding side information of MP3 signal is presented. And then frame with hidden message are estimated by using part2_3_length. That are describes in the following section.

3. MP3Stego

MP3 is one of the most popular audio formats on the Internet. MP3 provides a faithful reproduction of the original signal with a small amount of data, which enables it to be a desirable medium for covert communication. MP3Stego [3] exploits the degradation from lossy compression and embeds data by slightly expanding the distortion of the signal without attracting listeners' notice.

The MP3 audio encoding process is shown in Figure 2.

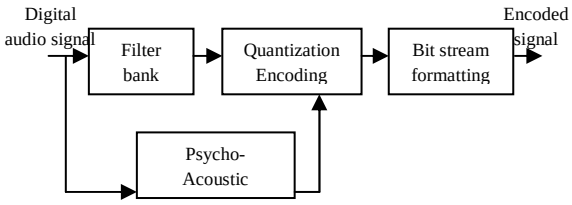


Figure 1. The MP3 Encoder

MP3Stego embeds compressed and encrypted data in the inner loop which is used for quantization and coding during MP3 coding.

In MP3Stego, the inner loop will continue to iterate until the parity of the part2_3_length is equal to the hidden bit and the bit demand for Huffman coding is also met. Once the inner loop is done, the outer loop will check the distortions introduced by the quantization operation. If the allowed distortion is exceeded, the inner loop will be called again. The above process will be iterated until the bit rate and distortion requirements are both met.

4. Proposed Steganography Detection and Message Length Extraction

This paper developed a MP3 steganalysis system to detect steganography or original signal. This system is adopted Principle Component Analysis (PCA) for steganography detection and Independent Component Analysis (ICA) for source separation.

ICA attempts to separate a set of observed signals that are composed of linear mixtures of a number of independent non-Gaussian sources into a set of signal that contain the independent source. This system requires the number of observed linear mixture input is at least equal to or larger than the number of independent sources. Mixture signal are generated by adding observed signal (X_1) and original signal (X_2) of audio file.

$$X = X_1 + X_2 \qquad (1)$$

The proposed steganography detection scheme is shown in Figure 2.

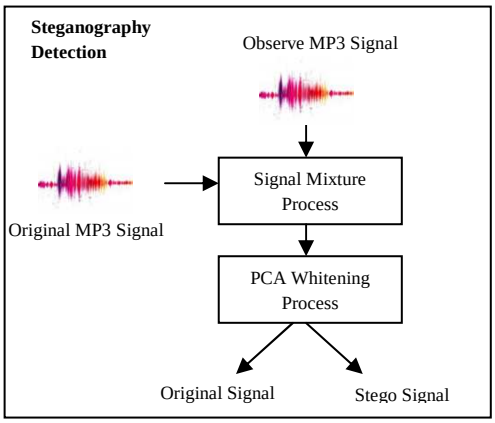


Figure 2. Block diagram of proposed Steganography Detection system

This signal is used for input data requirement of nonlinear blind extraction algorithm, robust batch ICA algorithm which is used for steganalysis process.

In signal mixture process, the observed signal mixes with similar MP3 signal. The mixture signal is entered into second stage to determine the original signal or stego signal by applying PCA (whitening process). Steganography detection system is

explained details in paper [17] that is one of my papers published in Singapore conference.

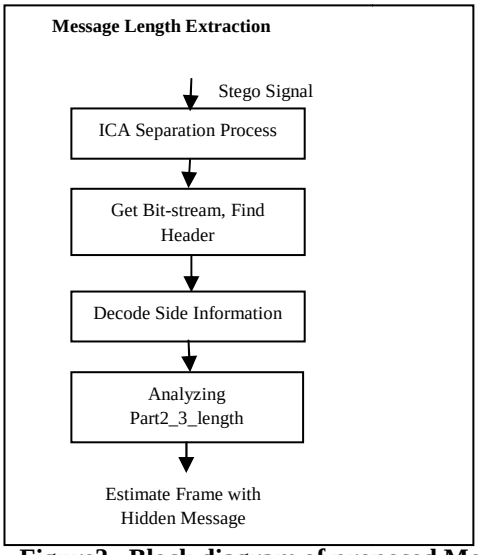


Figure3. Block diagram of proposed Message Length Extraction System

In the message length extraction system, the input signals contain hidden messages; use ICA separation method to separate the stego signals from the input signals. And then, extract bit stream of MP3 signal to calculate part2_3_length. As the result of part2_3_length value, hidden message length and frame with hidden message can be estimated.

4.1. Decoding Side Information of MP3 Signal

The side information is 17 bytes in length for a single channel encoded file and 32 bytes for dual channel mode. Data of Side Information allows decoding the main data correctly. Basic structure of side information is given in Figure 4:

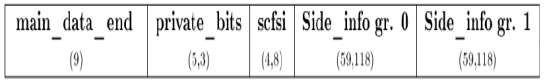


Figure4. Basic Structure of Side Information

Table 1 gives a clear picture of how the side information is organized both for single and dual channel modes. Organization of side information for block type 2 is presented in this table.

Table1. Organisation of side information for block types 0, 1 and 3

Name	Single channel	Dual channel
Main_data_begin	9	9
Private_bits	5	3
Share	4	4+4
Information for first granule:	12	12+12
Part2_3_length	9	9+9
Big_values	8	8+8
Global_gain	4	4+4
Scalefac_compress	1	1+1
Window_switching		
For normal blocks:		
Table_select	3*5	3*5+3*5
Region0_count	4	4+4
Region1_count	3	3+3
Subtotal for normal blocks	22	44
Preflag	1	2
Scalefac_scale	1	2
Count1table_select	1	2
Subtotal for first granule	59	118
Subtotal for second granule	59	118
Total number of bits	136	256
Total number of bytes	17	32

Lengths of each term mentioned in the tables are indicated in bits and terms involved in the tables 2.

Table2. Organisation of side information (block type 2)

Name	Single channel	Dual channel
For start, stop and short block:	2	2+2
Block_type	1	1+1
Mixed_block_flag	2*5	2*5
Table selection for two regions	2*5	+2*5
Subblock gain		3*3
		+3*3
Subtotal for not normal blocks	22	44

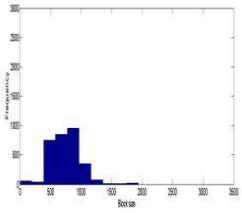
4.2. Estimating Frame with Hidden Messages

Part2_3_length contains the number of main_data bits used for scale factors and Huffman coded data. The main data is divided into two or four parts, for each granule and channel, depending on single or dual channel respectively. The size of each of these sections is the first item in the side information which is 12 bit unsigned integer.

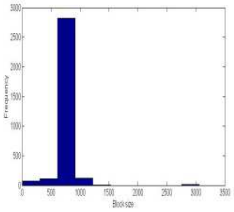
Table 3. Sample of part2_3_length Value from MP3 Files

Number of Frame	Part2_3_length of Stego	Part2_3_length of Original
1	[462;920;793;824]	[664;452;1092;663]
2	[730;763;759;707]	[866;562;955;528]
3	[775;722;432;1038]	[935;561;1079;555]
4	[903;781;590;678]	[919;564;915;654]
5	[740;927;828;817]	[928;567;975;596]
6	[754;766;586;806]	[859;520;854;493]
7	[618;967;674;917]	[831;477;846;522]
8	[827;793;348;904]	[804;510;811;462]
9	[730;950;702;857]	[778;520;838;515]
10	[710;778;442;1030]	[825;519;805;506]

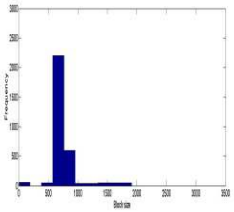
Table 2 shows that the values of part2_3_length are varied in stego and original MP3 signal. Therefore, frame with hidden message can be estimated by analyzing the part2_3_length of MP3 signals.



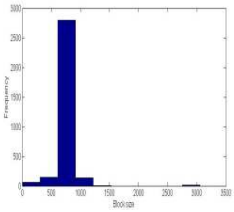
(a) Original signal for Blue



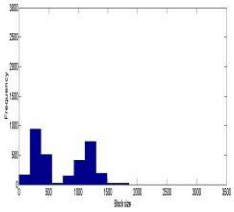
(b) Stego signal for Blue



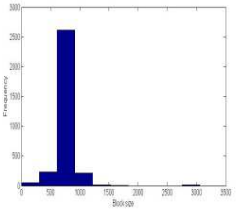
(c) Original Signal for Country



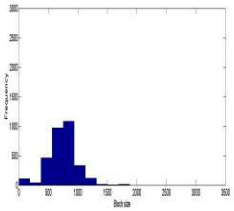
(d) Stego Signal for Country



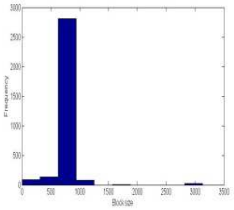
(e) Original Signal for R&B



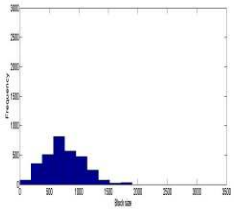
(f) Stego Signal for R&B



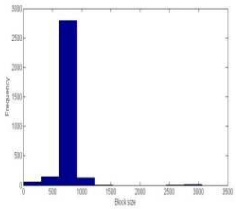
(g) Original Signal for Pop



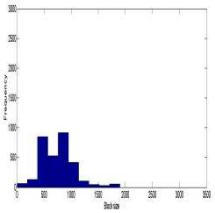
(h) Stego Signal for Pop



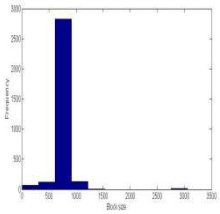
(i) Original Signal for Rock



(j) Stego Signal for Rock



(k) Original Signal for Rap



(l) Stego Signal for Rap

Figure 5. Histogram for Six Types of Music

In this figure, it can be seen that part2_3_length of stego signal are changed from the original signal. Block size between 500 and 1000, secret messages are embedded in this frame because block size is highly increased at nearly 3000 frequency. Therefore, frame with hidden message can be estimated by analyzing the part2_3_length value.

4.3. Analyzing Side Information with Various Compression Rate

Extraction part2_3_length and global_gain value from side information of detected signal. This process is done in MP3 decoding process. This section describes analyzing part2_3_length of MP3 file with compression rate 32kbps, 64kbps, 96kbps, 128kbps for highest amplitude rate of rock music file. Figure 6 presents the comparison for part2_3_length of MP3 file with 32kbps.

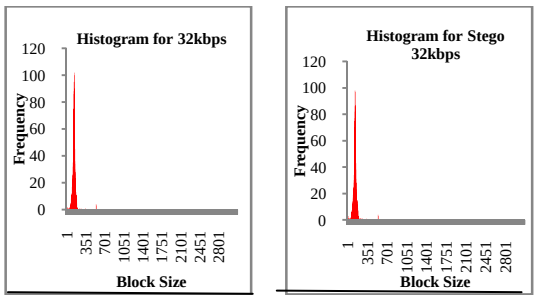


Figure 6. Comparison of part2_3_length over 32kbps Compression Rate (rock)

Figure 7 shows the comparison for part2_3_length of MP3 file with 64kbps. Block size (part2_3_length) are varied from the original MP3 files.

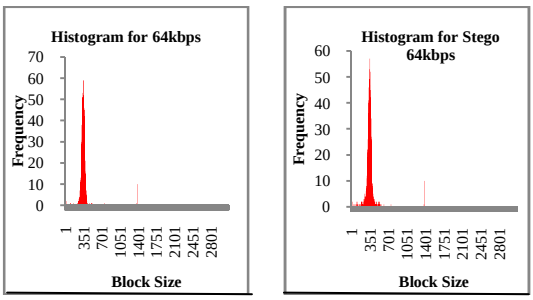


Figure 7. Comparison of part2_3_length over 64kbps Compression Rate (rock)

In this Figure 8, it can be seen that stego MP3 file is higher histogram ratio than original MP3 files. Below the point of histogram ratio are denser than original's histogram.

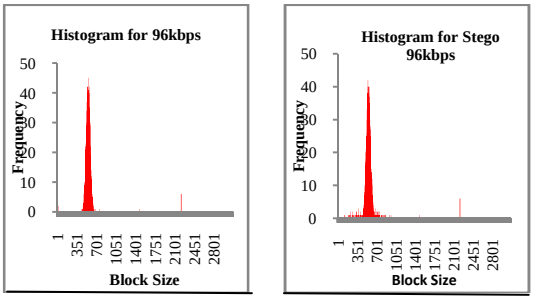


Figure 8. Comparison of part2_3_length over 96kbps Compression Rate (rock)

In MP3Stego tool, default bit rate is 128kbps for compression ratio of MP3 files. This compression ratio is tested in Figure 9. During my analysis, 20 sec MP3 file are compressed by various compression rates. It can be seen that default bit rate of MP3Stego compression is more embedded than other compression rate.

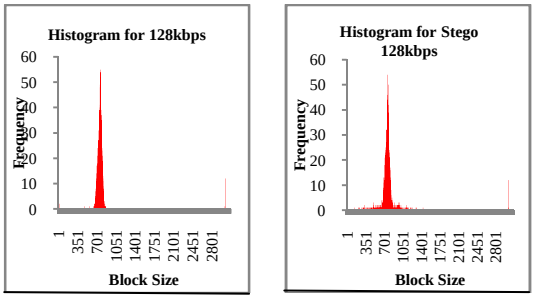


Figure 9. Comparison of part2_3_length over 128kbps Compression Rate (rock)

For example, 20 sec MP3 files are compressed by 128kbps that file carried more hidden messages than other compression rate. Figure 10 describes the maximum amount of hidden message are embedded in 20sec MP3 files. At that time, part2_3_length of stego signals are more varied than original signal. Because hidden message are embedded in every consecutive frame of MP3 file by MP3Stego.

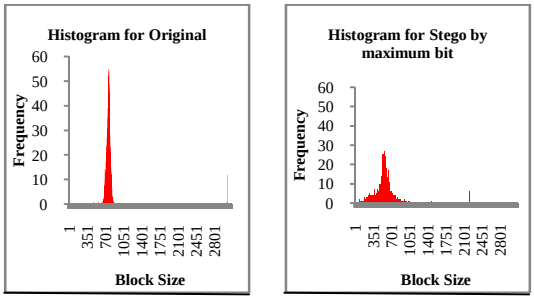


Figure 10. Comparison of part2_3_length over Maximum Amount of Secret Messages

5. Evaluation Results for Steganalysis System

In this section consists of two parts, the first one described the experimental set up of my proposed system and the latter one showed the performance analysis of steganography detection system.

5.1 Experimental set up

The propose steganalysis technique is implemented and tested on a set of 300 MP3 audio files. To evaluate the performance of proposed system, six types of MP3 signal (pop, blue, rock, rap, country, and r&b) are embedded by MP3Stego.Each audio has 20s interval and sampling amplitude is 44.1khz. This system produced the same amount of stego audio by hiding random messages in these audios. Then these MP3 files are detected and separated by PCA and ICA. Some signals cannot be detected by PCA because source signal and observed signal has same frequency rates.

While the PCA whitening process estimates the uncorrelated components, it is also quite useful to reduce the dimension of the data. In this application, reducing the dimension allows detecting whether the received signal is stego or not. If one of received audio streams is steganography, the PCA whitening automatically reduces the dimension to one. Figure 11 describes the detection accuracy under different number of bits. In MP3Stego, hidden message are compressed by zlib so this cause to vary detection accuracy over different bit numbers.

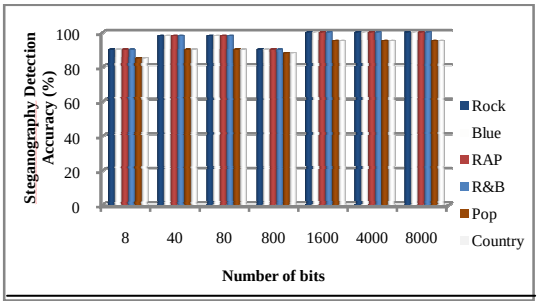


Figure 11. Detection Accuracy with different bit numbers

ICA performs decomposition on the whitened audio resulting that is estimated stego and original signal. ICA is used to separate the hidden message from original audio data by making process on the received observations. Then, calculate the correlation between hidden message with audio signal and pure audio signal.

As in robust batch algorithm, the optimum learning rule is derived based on decorrelation principle, where it is assumed that the sources are statistically independent, which implies that the cross-correlation is ideally zero. However, in practice the signals are not perfectly independent; hence it will degrade the separation performance.

Figure 12 demonstrates that the steganography has a high robustness against various noise levels. Above 30% of noise level, degrade the detection accuracy under 85%.

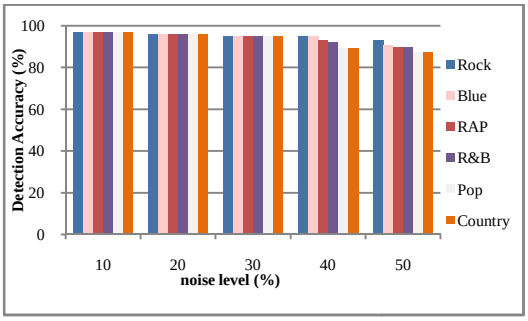


Figure 13. Detection Accuracy with different noise level

5.2 Performance results

In our experiments, receiver operating characteristic (ROC) curve has been used to verify the effectiveness of the proposed method. Figure 14 gives the ROC curves as the detection threshold Th is varied. It can be seen that maximum amount of bit are embedded in MP3 signal, true positive rate is nearly one and false positive rate is decreased.

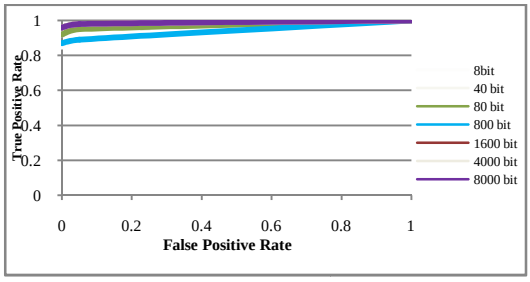


Figure 14. ROC curve under different bit numbers

6. Conclusion

In this paper, Independent Component Analysis (ICA) for audio steganalysis has been proposed. This system showed the efficacy and efficiency in applying ICA method for performing steganography detection and source separation. The steganography is readily detected by Principle Component Analysis (PCA) whitening process. By analyzing the nature of MP3 signals to estimate which MP3 frame have secret message bits. The performance of the proposed detection method can be evaluated in different bit numbers and MP3 files. The experimental result shows that the proposed method is useful for steganalysis of MP3Stego and to improve the accuracy of the detectors.

Reference

[1] N. F. Johnson, S. Jajodia. Exploring steganography: Seeing the unseen. IEEE Computer 31 (2),1988, 26 – 34.

[2] R. Chandramouli, M. Kharrazi, N. Memon. Image steganography and Steganalysis: Concepts and practices. International workshop on Digital Watermarking, 2004, 204 – 211.

[3] F. A. P. Petitcolas, MP3Stego, http://www.cl.cam.ac.uk/fapp2/steganography/mp3stego.

[4] C. Platt, UnderMP3Cover, http:// sourceforge.net/ projects/ump3c, 2004.

[5] Noch,Stego-Lame,http:// sourceforge.net/ projects/ stego-lame, 2002.

[6] A.Hyvärinen and E.Oja "Independent Component Analysis: Algorithms and Applications" Neural Networks Research Centre Helsinki University of Technology Neural Networks, 13(4-5):411-430, 2000

[7] A.H. Sung Novel Stream Mining for Audio Steganalysis ACM 978-1-60558-608-3/09/10 19th International Conference on Pattern Recognition.

[8] M. Qiao, A. Sung, Q. Liu, Steganalysis of MP3Stego, In: Proceedings of International JointConference on Neural Networks, Atlanta, Georgia, 2009, pp. 2566 – 2571.

[9] M. Qiao, A. Sung, Q. Liu, Feature mining and intelligent computing for MP3 steganalysis, In:Proceedings of International Joint Conference on

Bioinformatics, Systems Biology and IntelligentComputing, Shanghai, China, 2009, pp. 627 – 630.

[10] H. Ozer, B. Sankur, N. Memon, I. Avcibas, Detection of audio covert channels using statisticalfootprints of hidden messages, Digital Signal Processing, 16 (4) (2006), 389 – 401.

[11]C. Kraetzer , 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.

[12]Y.Huang, H.Song “Detecting MP3Stego and Estimating the Hidden Size” In Proceedings of the 20th International Joint Conference in Artificial Intelligence (IJCAI). 2808–2813.

[13]Q.Ding X. Ping “Steganalysis of Analysis-by-synthesis Compressed Speech” 978-0-7695-4258-4/10 $26.00 © 2010 IEEE DOI 10.1109/MINES.2010.148

[14] Hyv¨ arinen, A., Oja, E.: A fast fixed-point algorithm for independent component analysis. Neural Computation 9 (1997) 1483–1492

[15]Lee, T.W Independent Component Analysis: Theory and Applications. Kluwer Academic Publishers (1998)

[16]D.Yan, R.Wang “Steganalysis for MP3Stego using differential statistics of quantization step” Digital Signal Processing http:// dx.doi.org/10.1016/j.dsp.2013.02.013

[17]Y.Tint, K.T.Mya “Steganalysis for MP3Stego Using Independent Component Analysis”, 2013 International Conference of Information and Communication Technologies for Education.