International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Audio Features Based Steganography Detection in WAV File

Khin Myo Kyi

University of Computer Studies, Taungoo, Myanmar

How to cite this paper: Khin Myo Kyi "Audio Features Based Steganography Detection in WAV File" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1691-1694, **https://doi.org/10.31142/ijtsrd26807**

IJTSRD26807

ABSTRACT
Audio signals containing secret information or not is a security issue addressed in the context of steganalysis. ThRainfalle conceptual ide lies in the difference of the distribution of various statistical distance measures between the cover audio signals and stego-audio signals. The aim of the propose system is to analyze the audio signal which have the presence of information-hiding behavior or not. Mel- frequency ceptral coefficient, zero crossing rate, spectral flux and short time energy features of audio signal are extracted, and combine these features with the features extracted from the modified version that is generated by randomly modifying with significant bits. Moreover, the extracted features are detected or classified with a support vector machine in this propose system. Experimental result show that the propose method performs well in steganalysis of the audio stegnograms that are produced by using S-tools4.

KEYWORDS: *steganalysis, SVM, S-tools4*

1. Introduction
Steganography is to enable convert communication by hiding data in digital covers such as images, audios and videos, etc. Various steganography methods and software have been widely applied. Correspondingly, steganalysis techniques are developed to detect the existence of hidden information.

Steganalysis is the scientific technology to decide if a medium carriers some hidden messages or not and if possible, to determine what the hidden messages are.

There have been two main research approaches to the problem of steganalysis, namely, technique-specific steganalysis and universal steganalysis. The former group of techniques performs very accurately when used against the steganographic technique it is targeted for. The latter group of technique, on the other hand, are effective over a wide range of techniques, while performing less accurately overall. However, since universal steganalysis is better suited to the practical setting, it attracted more interest and many effective steganalyzers are proposed.

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. This paper focuses on WAV files. In order to discriminate stego audios from clear normal ones, that embed random data into a (possibly) stego WAV file by using a certain steganographic tool. It was found that the variation in some statistical features of WAV file is significantly different between clear WAV files and stego ones which already contain hidden mes-sages embedded by the same tool. In this paper, that can detect the existence of hidden messages, and also identify the tools used to hide them. As shown by the experimental results, the proposed method can be very effectively used to detect hidden messages embedded by StegoTool.

2. Related Work
In audio steganalysis, Christian Kraetzer and Jana Dittmann extended an existing information fusion based audio steganalysis approach by three different kinds of evaluations: The first evaluation addressed the so far neglected evaluations on sensor level fusion. The second evaluation enhanced the observations on fusion from considering only segmental features to combinations of segmental and global features. The third evaluation tried to build a basis for estimating the plausibility of the introduced steganalysis approach by measuring the sensibility of the models used in supervised classification of steganographic material against typical signal modification operations like de-noising or 128kBit/s MP3 encoding [3].

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 [1]. Andrew H. Sung investigated the use of chaotic-type features for recorded speech steganalysis. Considering that data hiding within a speech signal distorted the chaotic properties of the original speech signal, that designed a steganalyzer that used Lyapunov exponents and fraction of false neighbors as chaotic features to detect the existence of a stego-signal [5].

In this article, propose a steganalysis method of wav audios. Firstly, extract mel-frequency ceptral coefficient, zero crossing rate, spectral flux and short time energy features of the testing singnals. These systems employ learning classifier to discriminate the innocent audio signals and those carrying some hidden data.

3. Proposed framework of Audio Steganalysis

The proposed system adopted audio feature extraction in the audio steganalysis. In this process, different types of features are extracted from the observed audio signals that are detected by using support vector machine (SVM). Consequently a set of features for each training audio frame of the database is obtained, which are used to classify with observed audio features. The following figure 1 shows the process of proposed system.

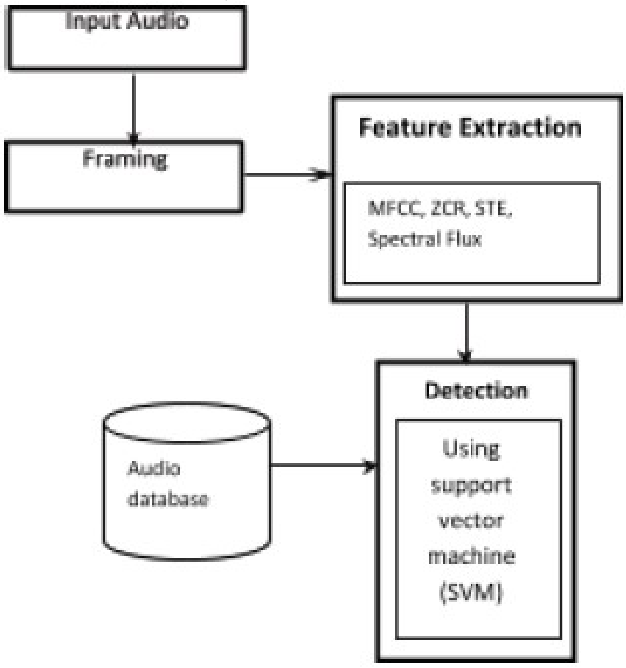

Figure 1 Process of Audio Steganalysis

In this study, different types of genres are used for testing and training audio. Audio signal are based on the different types of genres and steganography techniques. Two types of audio steganography techniques (StegoTool) is used in this steganalysis system.

4. Methodologies

4.1 Feature Extraction

The set of audio descriptors which has been developed are reviewed and used in audio signal processing. One of the most important parts of automated audio classification is the choice of features or properties. Features serve as the input to pattern recognition systems and are the basis upon which classifications are made. Most audio classification systems combine two processing stages: feature extraction followed by classification. In this paper, four types of features are computed from each frame, mel-frequency ceptral coefficient, zero crossing rate, spectral flux and short time energy of the testing and training signals.

4.1.1 Mel-Cepstral Domain based Features

Mel-frequency cepstral coefficients are non-parametric representations of audio signal, which models the human auditory perception system. The term "mel" is a unit of measurement of the perceived frequency or pitch of a tone. The mapping between the frequency scale (Hz) and the perceived frequency scale (mels) is approximately linear below 1 kHz and logarithmic at higher frequencies. The suggested formula that approximates this relationship is as follows

Fmel=2595.log101+FHz700 (1)

where Fmel is the perceived frequency in mels and FHz is the frequency in Hz.

The critical-band filters in the frequency domain (Hz) are illustrated in Figure (1). In the mel-frequency domain, the bandwidth and the spacing of these critical-band filters are invariable values, 300 mels and 150 mels, respectively.

The derivation of MFCCs is based on the powers of the theses critical-band filters. Let X(m) denote the power spectrum of an audio stream, S[k] denote the power in k-th critical band and M represent the number of the critical bands in mel scale, ranging usually from 20 to 24. Then

Sk=j=0f2-1Wkj.Xj, k=1,………,M (2)

Where Wk is the critical-band filter
Let L denote the desired order of the MFCC. Then we can find the MFCCs from logarithm and cosine transforms as follows

Cn=k=1Mlog Sk cos [k-0.5nπM], n=1,. (3)

4.1.2 Time Domain based Features

The well known short-term energy and zero-crossing rate (ZCR) are two popular choices in this category. ZCR measures the number of time domain zero crossings (divided by the frame's length).

If {x0,x1,……,xN-1} is the short term frame, then two features are given by

Short-term energy
E=1Nn=0N-1x2n (4)

Short-term zero crossing rate (ZCR)
ZCR=1Nn-1Nsgnxn-sgn{xn-1}2 (5)

Spectral Flux
A measure of the local spectral changed between successive frames. It is defined as the squared difference between these normalized magnitudes of the spectra of two successive frames:
FLt,t-1=k=0N-1(Ntk-Nt-1(k))2 (6)

Where
Ntk=Xtkt=0N-1XtL,Ntk (7)

Is the kth normalized DFT coefficient at the tth frame?

4.2 Steganography Detection with Support Vector Machine

SVM models the boundary between the classes instead of modeling the probability density of each class (Gaussian Mixture, Hidden Markov Models). SVM algorithm is a classification algorithm that provides state of the art performance in a wide variety of application domains. SVMs have been recently proposed as a new learning algorithm for pattern recognition. SVM learns an optimal separating hyper-plane from a given set of positive and negative examples.

Support Vector Machines (SVM) has recently gained prominence in the field of machine learning and pattern classification [8]. Classification is achieved by realizing a linear or non-linear separation surface in the input space. In Support Vector classification, the separating function can be expressed as a linear combination of kernels associated with the Support Vectors as

fx=xj∈SjyjK(xj,x)+b (8)

Where xi denotes the training patterns,yi∈{+1,-1} denotes the corresponding class labels and S denotes the set of Support Vectors.
The dual formulation yields

min0≤i≤CW=12i,jiQijj-ii+biyii (9)

Where i are the corresponding coefficients, b is the offset, Qij=yiyjK(xi,xj) is a symmetric positive definite kernel matrix and C is the parameter used to penalize error points in the inseparable case.

The Karush-Kuhn-Tucker (KKT) conditions for the dual can be expressed as

gi=∂Wi=iQijj+yib-1=yif(xi)-1 (10)

And
∂W∂b=jyjj=0 (11)

This partitions the training set into S the Support Vector set 0<i<C,gi=0,E the error set (i<C,gi<0)and R the well classified set (i=0,gi>0).

If the points in error are penalized with a penalty factor C', then, it has been shown that the problem reduces to that of a separable case with C=∞ . The kernel function is modified as
K'xi,xj=Kxi,xj+1C'ij (12)

where ij = 1 if i = j and ij = 0 otherwise. The advantage of this formulation is that the SVM problem reduces to that of a linearly separable case. It can be seen that training the SVM involves solving a quadratic optimization problem which requires the use of optimization routines from numerical libraries. This step is computationally intensive, can be subject to stability problems and is non-trivial to implement. Attractive iterative algorithms like the Sequential Minimal Optimization (SMO), Nearest Point Algorithm (NPA) etc. have been proposed to overcome this problem [8].

5. Evaluation Results for Steganalysis System

The proposed steganalysis technique is implemented and tested on a set of 400 wav files. The audio samples include songs (pop, blue, rap, country, rock and r&b) nature noise etc. These audio files are divided into four groups, 20 as normal audios, the remaining 60 included 30 Hide4PGP stego audios, and 30 S-Tools4 stego audios respectively embedded messages at 60% steganographic capacity with Hide4PGP and S-Tools4.

S-Tools is a steganographic tool that hides files in BMP, GIF, and WAV files. When it hides data in sounds, S-Tools distribute the bit-pattern corresponding to the file you want to hide across the least significant bits of the sound sample. S-Tools seed a cryptographically strong pseudo-random number generator from your passphrase and use its output to choose the position of the next bit from the cover data to use.

Figure 2 describes the detection accuracy under different number of bits which are tested with S-Tools.

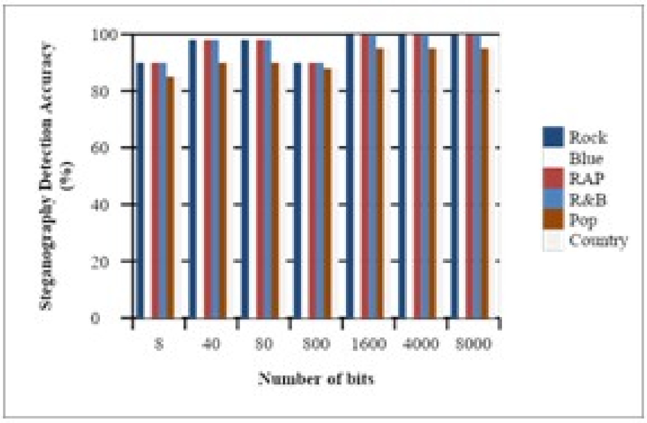

Figure2 Detection accuracy with different bit numbers

In this experiment, receiver operating characteristic (ROC) curve has been used to verify the effectiveness of the proposed method. Figure 3 gives the ROC curves as the detection threshold is varied. It can be seen that maximum amount of bit are embedded in signal, true positive rate is nearly one and false positive rate is decreased.

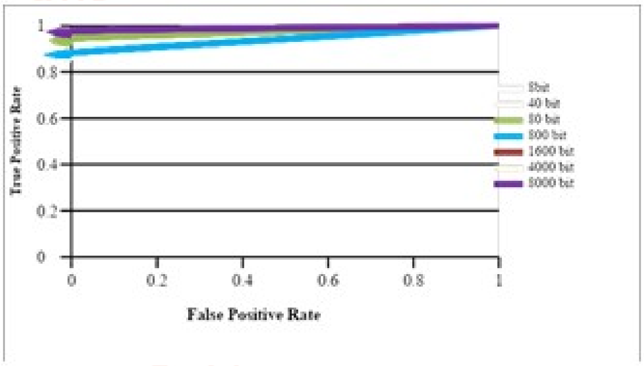

Figure 3 ROC curve under different bit numbers

6. Conclusion

Experimental results demonstrate that the proposed feature based steganalysis method performed well for different audio steganography tools as compared to various other existing methods. The proposed audio steganalysis method based on mel-frequency ceptral coefficient, zero crossing rates, short term energy and spectral flux are analyzed with SVM classification. Compared to the results of audio genres, country and pop songs have normal tone or low signal than other genres therefore which accuracy rate is little bit lower than others. Experimental results showed that proposed features based support vector machine is good in detecting the audio steganograms produced by using S-Tools 4 in digital WAV audios.

References

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

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

[3] 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.

[4] Jhing-Fa Wang Content- Based Audio Classification Using Support Vector Machines and Independent Component Analysis. 18th International Conference on Pattern Recognition (ICPR'06)

[5] 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

[6] S. Pfeiffer, S. Fischer, and W. E. Elsberg, "Automatic Audio Content Analysis," Tech. Rep. 96-008, Univ. Mannheim, Mannheim, Germany, Apr. 1996.

[7] Stools and A. Brown. (1996) S-Tools Version 4.0, CopyrightC. [Online]. Available: http://members.tripod.com/steganography/stego/s-tools4.html.

[8] S. Lyu, H. Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines," International Workshop on Information Hiding, Oct.2002, pp. 340-354.

[9] K. Wong and K. Tanaka "A Novel DCT-Based Steganographic Method Using Three Strategies," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, E91-A(10), 2008, pp.2897-2908.