POSTER: A Security Adaptive Steganography System Applied on Digital Audio

Xuejie Ding, Weiqing Huang, Meng Zhang(✉), and Jianlin Zhao

Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
{dingxuejie,huangweiqing,zhangmeng,zhaojianlin}@iie.ac.cn

Abstract. As a kind of covert communication technology, stegangoraphy can transmit cryptography using public cover on the internet. However, the behavior is easy to be found because of the cover distortion. To solve this problem, we define two distortion functions to measure the impact of embedding secret. They are called cover perception distortion (CPD) and statistical property distortion (SPD). Then a security stegangoraphy strategy can be generated adaptively by minimizing the two distortion functions. The experiment results demonstrate the effectiveness of our work.

Keywords: Steganography · Steganalysis · Distortion function · Modify path · Modify style

1 Introduction

Steganography can embed secret to the open cover such as images, audio and video in public communication mode without arousing suspicion. Compared with other kinds of multimedia, hiding data in audio is more challenging because of the sensitivity of human auditory system (HAS).

In the past years, several methods have been proposed based on the characteristics of digital audio signals and the human auditory system (HAS). Among the embedding algorithms, the least significant bits (LSB) substitution is one of the earliest techniques and used widely in audio and other media types. Hiding data in LSBs of audio samples can obtain the high data rate of embedding information, but it also faces challenges of various steganalysis system. So many kinds of algorithm based on LSBs have been proposed to improve the security with different transform domain or different embedding rules.

The goal of this paper is to design an audio steganography method which is more undetectable and imperceptibility. The novelty of this work is derived from distortion minimizing framework in image field [2]. We construct an embedding strategy includes security modify path and riskless modify style. They are established adaptively depends on minimizing two distortion functions. In details, first, every element in cover is assigned by the value of CPD, and then STCs is employed to find an optimal path. The elements belong to the modify path can be seen the less important parts according to CPD. Different from exiting distortion functions, the CPD is attained by an unsupervised algorithm. At last, SPD is used to determine the modify style for the elements on the path.

B. Thuraisingham et al. (Eds.): SecureComm 2015, LNICST 164, pp. 567–571, 2015.
DOI: 10.1007/978-3-319-28865-9_32

2 Proposed Method

The principle of novel steganography system is shown as follow, which can generate the embedding strategy adaptively for different covers.

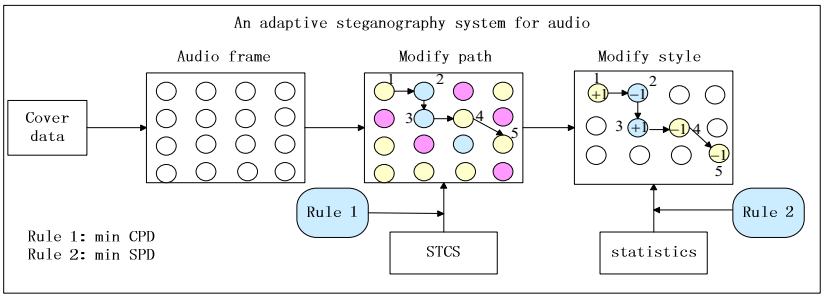


Fig. 1. The principle of novel steganography system

From Fig.1, we can see there are three key steps in the novel steganography system, they are depicted as follows.

Step 1(framing and DCT): We divide the audio cover $\boldsymbol{x}(t)$ into D non-overlapping frames $\boldsymbol{x}_i$, each frame is L samples. These DCT coefficients of each frame collectively form the new data matrix $\boldsymbol{X}=[\boldsymbol{X}(1),\cdots\boldsymbol{X}(D)]$.

Step 2 (Finding security modify path): A perception value is assigned for each element in cover, which represents the influence strength when the corresponding element is modified. The distortion function is defined as,

Rule 1:
$$MP(\boldsymbol{X},\boldsymbol{Y})=\arg\min D_{CPD}(\boldsymbol{X},\boldsymbol{Y}) \tag{1}$$

Then STCs [2] is employed to find a modify path which is subject to make the $D_{CPD}(\boldsymbol{X},\boldsymbol{Y})$ is minimal as Rule 1 describes. The theory of independent component analysis (ICA) is applied to construct CPD, and the procedure is shown in Fig. 2.

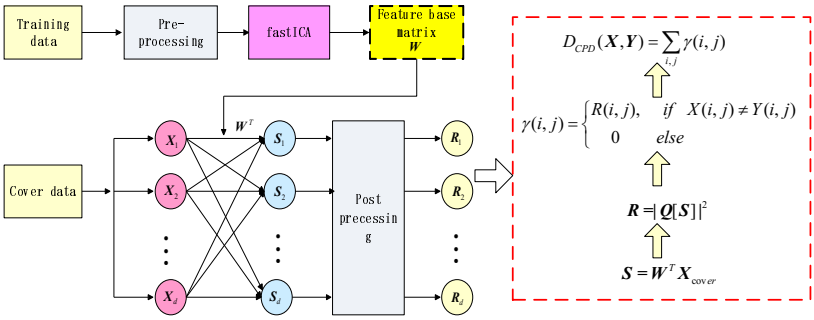
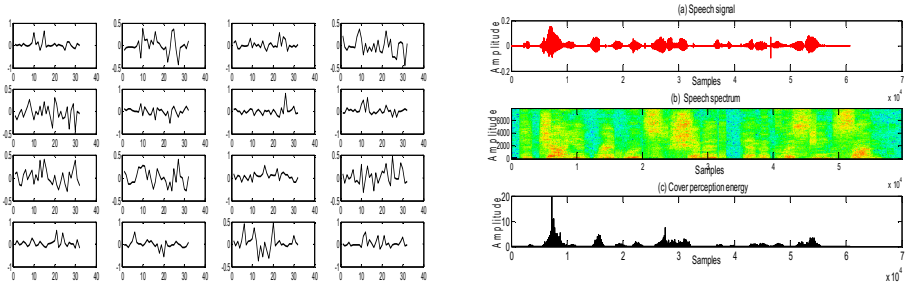


Fig. 2. The procedure of constructing CPD



(a) (b)

Fig. 3. Related results of CPD (a) Feature base matrix $\boldsymbol{W}$ (b) An example for distribution of cover perception energy.

Step 3 (Generating optimal modify strategy): The sender has to introduce modifications from cover $\boldsymbol{X}$ to stego $\boldsymbol{Y}$ at LSB. We design a distortion function to decide the modify style (-1 or $+1$) which is based on the statistical property of cover.

Rule 2:
$$MS(\boldsymbol{X},\boldsymbol{Y}) = \arg\min D_{SPD}(\boldsymbol{X},\boldsymbol{Y}) \tag{2}$$

The modify style is chosen when the $D_{SPD}(\boldsymbol{X},\boldsymbol{Y})$ is minimal as shown in rule2. Specially, generalized Gaussian distribution (GGD) is introduced to estimate the distribution of the DCT coefficients of each frame. The shape parameter is used to construct SPD as follows.

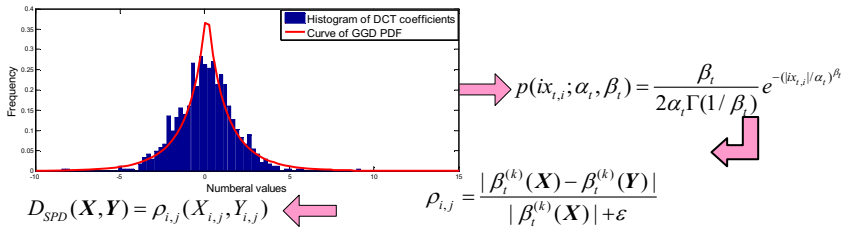


Fig. 4. The procedure of constructing SPD

The stego audio is attained after the inverse DCT of $\boldsymbol{Y}$. The secret can be extracted as (3) after the LSB of coefficients $\tilde{\boldsymbol{Y}}$ are extracted.

$$\tilde{\boldsymbol{Y}}\boldsymbol{H}^T = \boldsymbol{m} \tag{3}$$

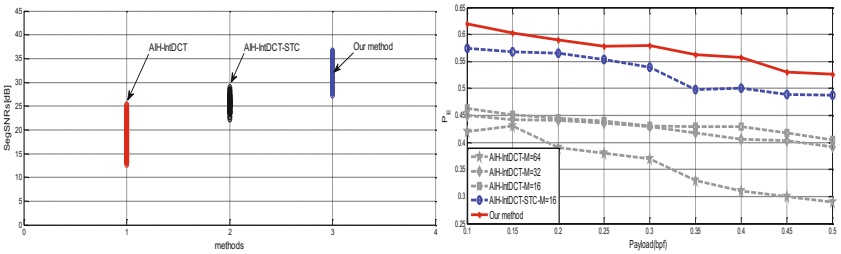
Where $\boldsymbol{H} \in \{0,1\}$ is the parity check matrix of the used STCs shared between sender and receiver.

3 Experimental Setup

We evaluate our algorithm using the dataset from TIMIT. The data is monophonic waveform with 16-kHz sampling. And the number of DCT coefficients in each frame is 1024. Our method is in comparisons with the algorithm in [1] used distortion function AIH-IntDCT (blocks M=16) and our improvement version exploited STCs. The security performance is evaluated as follows.

Table 1. Ratio of Score lower than 3.8 evaluated by PESQ

Payload (bpf)	Algorithms		
	AIH-IntDCT	AIH-IntDCT-STC	Our method
0.1	2.2%	0	0
0.2	3%	0.8 %	0
0.3	4.5%	0.9%	0.52%
0.4	12.5%	8.2%	7.2%
0.5	13.5%	9.6%	7.4%



(a) (b)

Fig. 5. Objective evaluation results: (a) SegSNRs results at payload 0.5 (b) Steganalysis results using CC-PEV features in [3].

4 Conclusion

With the motivation to improve security, two distortion functions have been constructed to measure the impact of embedding secret. They guide the embedding positions and strategy respectively. Experiment results have shown that our method has good performance with lower distortion and larger error detection.

Acknowledgement. This work is supported by the "Strategic Priority Research Program" of the Chinese Academy of Sciences, Grant No. Y2W0012306.

References

1. Huang, X., Ono, N., Echizen, I., Nishimura, A.: Reversible audio information hiding based on integer DCT coefficients with adaptive hiding locations. In: Shi, Y.Q., Kim, H.-J., Pérez-González, F. (eds.) IWDW 2013. LNCS, vol. 8389, pp. 376–389. Springer, Heidelberg (2014)
2. Filler, T., Judas, J., Fridrich, J.: Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. IEEE Trans. Inf. Forensics Security **6**(3), 920–934 (2011)
3. Kondovsky, J., Fridrih, J.: Calibration revisited. In: Proceedings of the 11th ACM Multimedia and Security Workshop, Princeton, NJ, September 7–8, 2009