

# Overview of Audio Watermarking Algorithm against Synchronization Attacks

Haiyan Liu and Wuyi zhang

Department of Computer Engineering, Beijing Information Technology College, Beijing 100018, China

**Abstract**—T Synchronization is the one of the most important issues in digital audio watermarking algorithms. This paper describes the audio watermarking algorithms against synchronization attacks, introduces the advantages and disadvantages of each algorithm in detail. The article finally discusses the existing problems of current algorithms and the problems solved.

**Keywords**- audio watermarking; synchronization; exhaustive search method; display synchronization; implicit synchronization

## I. INTRODUCTION

With the rapid development of Internet and digitalization of media resources, the piracy problem of images, audio, video is increasingly outstanding so that the digital watermarking technology has become an important research focus and caused attention of scholars in the field of the information security, computer technology and information processing.

The watermarking mainly refers to the specific information is embedded into the digital work to prove the ownership of digital works or to track violations. The digital watermarking technology makes up the shortcomings of traditional cryptography on security protection of multimedia content and has become an important means of digital media copyright protection [1].

Digital audio watermarking algorithms mainly protect the copyright protection, piracy tracking and certification of audio signal. In recent years, robust audio watermarking technologies has improved greatly, however, the ability to attack for digital watermarking is getting stronger, especially, the synchronization attacks. The paper mainly summaries the digital audio algorithms against synchronization attacks.

The methods against synchronization attacks include the exhaustive search scheme, display synchronization scheme, autocorrelation scheme, invariant watermark scheme, implicit synchronization scheme. In this paper, the article introduces the type of synchronization attacks, analyzes the advantages and disadvantages of the methods, describes the audio watermarking algorithm against synchronization attacks in details, discusses the existing problems and development of algorithms against synchronization attacks.

## II. THE TYPE OF SYNCHRONIZATION ATTACKS

Anti-attack ability is one of the most important performance indicators of the digital watermarking system. The attacks of audio watermarking mainly attack the audio watermarked to destroy the embedded watermark information and to cause the

users can not properly extract the watermark information or extract the wrong watermark information. According to the influence of synchronization structure of the audio signal, the attacks can be divided into conventional attacks and synchronization attacks. Conventional attacks occur mainly in the process of network channel transmission, lead to lower audio quality because of the signal interference, but the audio signal synchronization Structure doesn't change which include Re-quantization, Re-sampling, Echo addition, Mp3 compression, Noise addition, Equalization, Pass filtering. The synchronization attack does not completely remove the watermark information, but only disable the synchronization between the watermark and the detector. The watermarking information embedded in the audio attacked still exists and the amplitude does not be changed, but the watermark has been misplaced, the detection algorithm can not correctly extract the watermark information. The types of attack include pitch-shift warping, jittering attack, amplitude variation, dropping, random removal, random duplication, Time-scale modification ( TSM), D/A and A /D conversion.

- Random Cropping: Random cut 15% audio signal in front of the digital audio signal (or middle, back)

- Amplitude variation: The amplitude value of the digital audio signal is amplified to 150% or reduced to 50%.

- Time-Scale Modification: The entire length of the digital audio is extended  $\pm 11\%$  under the pitch remains unchanged.

- Dropping: firstly, the dropping attack divides the entire audio signal into n data blocks of audio samples, and then copies or deletes a audio sample in each data block random, finally the data blocks are re-combined according to the original order.

## III. AUDIO WATERMARKING ALGORITHMS AGAINST SYNCHRONIZATION ATTACKS

### A. Exhaustive Search Method

The exhaustive search method is the easiest way to recovery of the watermark after the audio signal suffers from synchronization attacks in time domain. By the defining the range and the step size of relevant parameters (such as time scaling and delay), their combinations represent an attack to the audio signal already undertaken. Each possible combination is reversed firstly when watermark is detected, and then the watermark detector is applied for each detection.

The exhaustive search method causes two major problems: (1) the computational cost increases rapidly with the

increasing of search space; (2) the multiple operations of watermark detector will increase the false alarm rate. So, the exhaustive search method is effective when the search space is small.

In [2], a self-synchronization audio watermarking algorithm was proposed. The algorithm achieved self-synchronization by searching all the sampling points of the target frame. The watermark detection blind detection.

#### *B. Display Synchronization Scheme*

The display synchronization method embeds synchronization data except embedding the watermark information. The synchronization data is named synchronization flag. The synchronization flags generally use m-sequence or Barker code. Using the method, the detection algorithm finds the synchronization flags, compares these flags with the embedded flags to identify the attacks which the audio signal is suffered, detects the watermark information after the attacks are reversed.

In [3], the algorithm embedded synchronization signals in the time domain to resist the attacks such as cropping while keeping the computation for resynchronization being lower. The experimental results show that the hidden imperceptible watermark was robust to the attacks caused by additive noise, MP3 coding, and cropping.

In [4], the scheme adopted the barker code with special autocorrelation function as synchronization flags.

In [5], the scheme embedded the synchronization codes and the watermark information into the low frequency coefficients in discrete wavelet transform domain. By exploiting the time-frequency localization characteristics of DWT, the computational load in searching synchronization codes had been reduced, thus resolving the contending requirements between robustness of hidden data and efficiency of synchronization codes searching.

In [6], a novel synchronization approach applying passive audio fingerprinting to synchronize each watermarking bit individually. Storage of the fingerprint values is not necessary in the approach, improving the usability compared to existing solutions.

This approach causes three problems: (1) The embedding of the synchronization data increase the embedding capacity to decrease the quality of the audio signal; (2) It is very easy to produce the false alarm rate; (3) It is very easy to cause the security issues. In general case, the same synchronization flag is used to a series of different audio signals, which eases the task of the detector but can be easily found and removed by the attackers.

#### *C. Autocorrelation Scheme*

In some cases, some embedded data with autocorrelation property can be simultaneously used as synchronization data and load data. Autocorrelation function has a large peak at zero point and decreases rapidly to zero at non-zero point. The autocorrelation mode is similar to add a synchronization flag.

#### *D. Invariant Watermark Scheme*

By nature, the invariant watermark is to use the physical quantity which audio signal is not sensitive to various attacks to embed hiding information.

In [7], a synchronization invariant audio watermarking scheme based on the statistical feature manipulation in wavelet domain was proposed. The experimental results demonstrated that this algorithm was robust to common attacks, pitch shifting, random cropping, and time-scale modifications.

In [8], A robust and blind audio watermarking algorithm based on the discrete wavelet transform (DWT) was proposed. The algorithm embedded the watermark information into the absolute average of audio low frequency coefficients in the DWT and error- correcting coding was applied in order to lower the bit error rate of watermark in extraction. Experimental results show the performance of the method was ideal against various common signal processing attacks, especially, robustness to de-synchronization attacks.

In [9], based on the property that the statistical mean value of 4th level wavelet coefficients was next to zero, a bit watermarking was embedded into the audio segment, by modifying the statistical mean value of the 4th level detail wavelet coefficients. The simulated experimental results proved that the algorithm was robust.

In [10], the statistical-mean manipulation method was used to achieve the invariant watermarking according to the feature of cep-strum coefficients. The simulation results proved the effectiveness of the scheme.

In [11], taking use of the feature that relative gravity of center of audio was steady and was insensitive to Time-Scale Modification operation and other synchronization attacks to generate the watermark information. The encrypted watermark was embedded into the third level wavelet approach coefficients of audio by quantification method. Experiment results showed that the scheme had good robustness that could resist common signal processing and 20% TSM, 1/10 dithering manipulation.

#### *E. Implicit Synchronization Scheme*

Implicit synchronization is that the actual feature of carrier is used to identify the watermark embedding position, these feature points and the watermark information can be detected together. The type of algorithms depend on the invariance property of these features, and therefore the feature points may be higher regions of the audio signal energy or higher regions of zero-crossing rate, such as zero-crossing rate, pitch, tempo, frequency centroid. Implicit synchronization is the better strategy of resisting synchronization attacks, however, the scheme relies on the content of the audio signal, the audio signal which does not meet the requirements can not use this method.

In [12], the psychoacoustic model was used to ensure the imperceptibility of the embedded watermark. The watermark was hid in the Discrete Cosine Transform (DCT) domain by changing the phase of five information carriers determined using the psychoacoustic model. Blind detection was realized

through the application of a novel synchronization scheme, the peak point extraction (PPE) scheme. Experimental results showed that the algorithm was robust against various attacks such as cropping and re-sampling

In [13], the paper presented an audio watermarking algorithm against synchronization attacks by changing the length of the intervals between salient points of the audio signal to embed data. The intervals were quantized and the watermark information was embedded in the quantization indices. The paper used the wavelet of the signal envelope as the salient point and proposed novel ideas for practical implementation that could be used by other data embedding schemes as well. The system was robust to mp3 compression, low pass filtering, sampling rate conversion, and time-scale modification (TSM).

In [14], according to support vector regression (SVR), the adaptive digital audio watermarking algorithm was presented which need not the original audio signal when the watermark was detected. This algorithm embedded the template information and watermark signal into the original audio by adaptive quantization according to the local audio correlation and human auditory masking. Experimental results showed that the audio watermarking scheme was not only imperceptible, but also robust against various common signal attacks and synchronization attacks.

In [15], a self-synchronization blind audio watermarking in DWT was presented based on  $(t, n)$  threshold. The scheme used the features of the audio signal transferred to embed the watermark information.

In [16], the authors presented the algorithm against synchronization attacks based on character of dual-channel audio which computed the Mel frequency spectrum coefficient and used the correlation between left and right channel. The watermark information was embedded into synchronized segment in left and right channel at the same time. The simulation results showed that the approach had good robustness.

In [17], the author took use of the audio cep-strum domain and energy features to decide the regions of embed frames. The simulation results proved the scheme is effective to resist common proceeding and synchronization attacks.

In [18], the paper proposed a digital audio watermarking algorithm which can resist the random cropping and TSM attacks based on the local statistical features of audio signal. Firstly, the approach divided the original audio into segments. Secondly, the histogram and the absolute mean value of each segment were computed to embed the watermark information. The experimental results proved the proposed algorithm could provide good performance for random cropping and TSM attacks.

#### IV. SUMMARY

In summary, the audio watermarking schemes of anti-sync attacks have solved the problems as follows: (1) most of the watermark algorithms take into account the human auditory system when the watermark information is embedded so that

the imperceptibility of system is improved; (2 ) Most of algorithms achieves blind detection (3) Most of algorithms can resist one or several synchronization attacks. However, in terms of resistance to synchronize attacks, there are some defects:

In summary, the audio watermarking schemes of anti-sync attacks have solved the problems as follows: (1) most of the watermark algorithms take into account the human auditory system when the watermark information is embedded so that the imperceptibility of system is improved; (2) Most of algorithms achieves blind detection; (3) Most of algorithms can resist one or several synchronization attacks. However, in terms of resistance to synchronize attacks, there are some defects [11]:

1) The algorithms of anti-synchronized attacks is just designed for a certain kind of attack and can not resist many types of synchronization attack. Such as, in [19], the proposed method resisted only cutting attacks and cut slices attacks;

2) Most of the existing synchronization algorithms is based on synchronization strategy of sample alignment. It is very difficult to keep the strict alignment when the systems are attacked by TSM, random cutting .

#### ACKNOWLEDGMENT

The National Natural Science Foundation of China(No. 61370092) science and Technology Project of Beijing Municipal Commission of Education Natural Science(No.KM201310857001).

#### REFERENCES

- [1] Cox I J, Miller M L, Bloom J A. Digital Watermarking[M]. Morgan Kaufman Publishers, 2002.
- [2] Shuifa Sun, Sam Kwong. A Self-synchronization Blind Audio Watermarking Algorithm [A]. In: Proceeding of 2005 International Symposium on Intelligent Signal Processing and Communication Systems[C], 2005: 133~136.
- [3] Huang J W, Wang Y, shi Y Q. A blind audio watermarking algorithm with self-synchronization.[A] IEEE International Conference on Circuits and Systems[C]. 2002. 627-630.
- [4] XiangYang Wang, Hong Zhao. A Novel Synchronization Invariant Audio Watermarking Scheme Based on DWT and DCT [J]. IEEE Transactions on Signal Processing, 2006, 54(12): 4835~4839.
- [5] Shaoquan WuJiwu Huang,Daren Huang Shi, Y.Q.Efficiently self-synchronized audio watermarking for assured audio data transmission [J], Broadcasting, IEEE Transactions on, March 2005, Volume: 51,Issue: 1, pp. 69- 76
- [6] Martin Steinebach and Sascha Zmudzinski, Blind audio watermark synchronization by passive audio fingerprinting[J] Proceedings of SPIE ,Vol. 6505, Feb. 27, 2007, pp.509-518
- [7] Li W, Xue X Y, Audio watermarking based on statistical feature in wavelet domain. Proc.of Poster Track of the Twelfth International World wide web conference Budapest, Hungary,May 2003.
- [8] Liu Haiyan, Zheng Xuefeng, Wang Ying. DWT-Based Audio Watermarking Resistant to Desynchronization. IEEE 7th International Conference on Computer and Information Technology.2007:745~748.
- [9] Huang Xionghua, Jiang WEizhen. Robust Audio Blind Watermarking of Discrete Wavelet Transform Based on Chaos. Journal of Chengdu University (Natural Science Edition), 2009, 28(4): 318-321.
- [10] Nian Guijun, Wang shuxun, Tang xiaonian. Robust Adaptive Audio Watermarking Algorithm in Cepstrum. Journal of Jilin University(Information Science Edition), 2008, 26(1): 55-61.

- [11] Huang xionghua, Wang hongxia, Jing weizhen, Cui gengshen. Audio Watermarking Algorithm Against Synchronization Attacks Based on Gravity of Center. ACTA AUTOMATICA SINICA, 2013, 39(8): 1321–1329.
- [12] Foo Say Wei, Feng Xue, Mengyuan Li. A Blind Audio Watermarking Scheme Using Peak Point Extraction [J]. IEEE International symposium on Circuits and Systems, 2005, 5: 4409~4412.
- [13] Mansour M, Tewfik A. Data embedding in audio using time-scale modification. IEEE Trans Speech Audio Process, 2005, 13(3): 432–440.
- [14] Wang XY, Qi W, Niu PP. A new adaptive digital audio watermarking based on support vector regression. IEEE Trans On Audio Speech Lang Process, 2007, 15(8): 2270–2277.
- [15] Zhang li, Chen limin, Xiao weiwei. Self-synchronization blind audio watermarking based on (t,n) threshold. Journal of Shenzhen University science and engineering, 2006, 23(3): 252–257.
- [16] Feng tao, Han jiqing. Synchronization and blind detect algorithm for dual channel audio watermark. Journal of Communications, 2006, 27(10): 62–68.
- [17] Li jian. A Robust Implicit Synchronization Algorithm of Digital Audio Watermarking. Computer Engineering and Applications, 2004, 40(10): 72–74.
- [18] Xiang shijun, Huo yongjin, Liu shangyi, Luo xinrong. Audio Watermarking against Synchronization Attacks Using statistical Features. JOURNAL OF APPLIED SCIENCES — Electronics and Information Engineering, 2014, 32 (4): 434–440.
- [19] Liu xiuying, Duan xiaoyi, Wang jianxin. Audio Watermarking scheme with Self-synchronization based on Psychoacoustic Model. Computer Engineering and Applications, 2013, 49(8): 96–99.