High Capacity FFT-Based Audio Watermarking

Mehdi Fallahpour, David Megias

HAL Id: hal-01596185
https://hal.inria.fr/hal-01596185

Submitted on 27 Sep 2017

High capacity FFT-based audio watermarking

Mehdi Fallahpour and David Megías

Estudis d'Informàtica, Multimèdia i Telecomunicació
Internet Interdisciplinary Institute (IN3)
Universitat Oberta de Catalunya, Barcelona, Spain

E-mail: {mfallahpour,dmegias}@uoc.edu

Abstract. This paper proposes a novel high capacity audio watermarking algorithm to embed data and extract it in a bit-exact manner based on changing the magnitudes of the FFT spectrum. The key idea is to divide the FFT spectrum into short frames and change the magnitude value of the FFT samples based on the average of the samples of each frame. Using the average of FFT magnitudes makes it possible to improve the robustness, since the average is more stable against changes compared with single samples. In addition to good capacity, transparency and robustness, this scheme has three parameters which facilitate the regulation of these properties.

Considering the embedding domain, audio watermarking techniques can be classified into time domain and frequency domain methods. In frequency domain watermarking [1-7], after taking one of the usual transforms such as the Discrete/Fast Fourier Transform (DFT/FFT) [4-6], the Modified Discrete Cosine Transform (MDCT) or the Wavelet Transform (WT) from the signal [7], the hidden bits are embedded into the resulting transform coefficients. In [4-6], which were proposed by the authors of this paper, the FFT domain is selected to embed watermarks for making use of the translation-invariant property of the FFT coefficients to resist small distortions in the time domain. In fact, using methods based on transforms provides better perceptual quality and robustness against common attacks at the price of increasing the computational complexity.

In the algorithm suggested in this paper, we select the middle frequency band of the FFT spectrum (4–12 kHz) for embedding the secret bits. The selected band is divided into short frames and a single secret bit is embedded into each frame. Based on corresponding secret bit, all samples in each frame should be changed by the average of all samples or the average multiplied by a factor. If the secret bit is "0", all FFT magnitudes should be changed by the average of all FFT magnitudes in the frame. If the secret bit is "1", we divide the FFT samples into two groups based on the sequence and, then, we change the magnitude of the first group using a scale factor, α, multiplying the average of all samples and the magnitude of the second group multiplying $(2 - \alpha)$ by the average. These changes both in embedding "0" or "1", keep the average of the frame unchanged after embedding. Using the average of a frame is very useful to increase the robustness against attacks, whereas embedding a secret bit into a

single sample is usually fragile. In addition, using FFT magnitudes, sqrt(real^2 + imag^2), results in better robustness against attacks compared to using the real or the imaginary parts only.

The Objective Difference Grade (ODG) has been used to evaluate the transparency of the proposed algorithm. The ODG is one of the output values of the ITU-R BS.1387 PEAQ standard, where ODG = 0 means no degradation and ODG = –4 means a very annoying distortion. Additionally, the OPERA software based on the ITU-R BS.1387 has been used to compute this objective measure of quality.

The experimental results show that this method achieves a high capacity (about 0.5 to 4 kbps), provides robustness against common signal processing attacks and entails very low perceptual distortion (ODG is about –1). The proposed scheme is robust against several attacks such as AddDynNoise, ADDFFTNoise, Addnoise, AddSinus, Amplify, Invert, LSBZero, RC_HighPass, and RC_LowPass of the Stirmark Benchmark for Audio [9]

The method proposed in this paper has been compared with several recent audio watermarking strategies. Almost all the audio data hiding schemes which produce very high capacity are fragile against signal processing attacks. Because of this, it is not possible to establish a comparison of the proposed scheme with other audio watermarking schemes which are similar to it as capacity is concerned. Hence, we have chosen a few recent and relevant audio watermarking schemes in the literature. We compare the performance of the proposed watermarking algorithm and several recent audio watermarking strategies robust against the MP3 attack. [1, 8, 2, 4, 3] and the proposed scheme have capacity equal to 2, 2.3, 4.3, 2996, 689, and 506 to 4025 (bits per second) respectively, also transparency in term of Objective Difference Grade (ODG) is (–1.66 to –1.88), Not reported, Not reported, –0.6, Not reported and (–0.1 to –1.5).

[1, 2, 8] have low capacity but are robust against common attacks. [3] Evaluates distortion by using the mean opinion score (MOS), which is a subjective measurement, and achieves transparency between imperceptible and perceptible but not annoying (MOS = 4.7).

Capacity, robustness and transparency are the three main properties of an audio watermarking scheme. Considering a trade-off between these properties is necessary. E.g. [1] proposed a very robust, low capacity and high distortion scheme. However [3] and the proposed scheme lead to high capacity and low distortion but they are not as robust as the low-capacity method described in [1]. The scheme presented in [4], which was also proposed by the authors of this paper, has good properties, but the scheme proposed in this paper can manage the needed properties better since there are three useful adjustable parameters. For example, in the proposed scheme by using a frame size of $d = 8$ getting robustness against MP3–64 is straightforward. On the other hand, in [4], low bit rate MP3 compression was not considered.

In short, we present a high-capacity watermarking algorithm for digital audio which is robust against common audio signal processing. A scaling factor, the frame size and the selected frequency band are the three adjustable parameters of this method which regulate the capacity, the perceptual distortion and the robustness of the scheme accurately. Furthermore, the suggested scheme is blind, since it does not need the original signal for extracting the hidden bits.

The experimental results show that this scheme has a high capacity (0.5 to 4 kbps) without significant perceptual distortion and provides robustness against common signal processing attacks such as added noise, filtering or MPEG compression (MP3).

References

1. Xiang S., Kim H.J., Huang J., "Audio watermarking robust against time-scale modification and MP3 compression," *Signal Processing*, Vol. 88 No.10, pp.2372-2387, October, 2008.
2. Mansour M. and Tewfik A., "Data embedding in audio using time-scale modification," *IEEE Trans. Speech Audio Process.*, Vol. 13, No. 3, pp. 432–440, 2005.
3. Garcia-Hernandez J. J., Nakano-Miyatake M. and Perez-Meana H., "Data hiding in audio signal using Rational Dither Modulation", *IEICE Electron. Express*, Vol. 5, No. 7, pp. 217-222, 2008.
4. Fallahpour M., Megías D., "High capacity audio watermarking using FFTamplitude interpolation" *IEICE Electron. Express*, Vol. 6, No. 14, pp. 1057-1063, 2009.
5. Fallahpour M., Megías D., "High Capacity Method for Real-Time Audio Data Hiding Using the FFT Transform", Advances in Information Security and Its Application, Springer-Verlag. pp. 91-97, 2009.
6. Fallahpour M., Megías D., "Robust high-capacity audio watermarking based on FFT amplitude modification" *IEICE Trans on Information and Systems,* Vol.E93-D, No.01, pp.87-93, Jan. 2010.
7. Fallahpour M., Megías D., "DWT–based high capacity audio watermarking", *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences,* Vol.E93-A, No.01, pp.331-335, Jan. 2010.
8. Li W., Xue X., "Content based localized robust audio watermarking robust against time scale modification" *IEEE Trans. Multimedia*, Vol. 8, No. 1, pp. 60-69, Feb. 2006.
9. Stirmark Benchmark for Audio. http://wwwiti.cs.uni-magdeburg.de/~alang/smba.php