Audio watermarking: features, applications and algorithms

Conference Paper · February 2000

DOI: 10.1109/ICME.2000.871531 · Source: IEEE Xplore

1 author:

Michael Arnold
Leibniz School of Business
27 PUBLICATIONS **592** CITATIONS

SEE PROFILE

AUDIO WATERMARKING: FEATURES, APPLICATIONS AND ALGORITHMS

Michael Arnold

Department for Security Technology for Graphics and Communication Systems
Fraunhofer-Institute for Computer Graphics
64283 Darmstadt, Germany
arnold@igd.fhg.de

ABSTRACT

This paper considers desired properties and possible applications of audio watermarking algorithms. Special attention is given to statistical methods working in the fourier domain. It will present a solution of robust watermarking of audio data and reflect the security properties of the technique. Experimental results show good robustness of the approach against MP3 compression and other common signal processing manipulations. Enhancements of the presented methods are discussed.

1. INTRODUCTION

The problems associated with copyright protection, i.e. the protection of intellectual property rights (IPR), arise from the transition from analog to the digital data representation. Easy copying with a bit-by-bit reproduction of original and all copies, simple and inexpensive distribution of information across networks with the help of compression mechanisms causes new problems. In the case of audio data personalized audio players are often used to establish a usage control. The control over the data is lost if it emerges from such secured envirionements. An other idea of the protection of IPR, also known as watermarking, is to integrate information relevant to the IPR directly into the data.

2. DESIRED FEATURES OF AUDIO WATERMARKING ALGORITHMS

From a general point of view a watermark establishes a link between the raw data and corresponding information. This link can serve different purposes. Therefore the different kind of watermarks are categorized as:

Secret watermarks can be used as authentication and content integrity mechanisms in a variety of ways. This implies that the watermark is a secured link readable only by authorized persons with the knowledge about the secret.

Public watermarks act as an information carrier with the watermark readable by everybody. These public watermarks should be not detectable or removable by a third party. This requirement can be lowered if these watermarks act as information links.

According to the intention and the kind of watermark, watermarking techniques should possess certain signal, security and general properties.

Signal processing properties

- The watermark should be not perceivable by an observer.
- The watermark should be robust against intentional or anticipated manipulations, e.g. compression, filtering, resampling, requantisation, cropping, scaling, etc.

Security properties

- The watermarking procedure should rely on a key to ensure security, not on the algorithm's secrecy [6].
- The algorithm should be published.
- The watermark should be statistically undetectable.
- The algorithm should have a mathematical formulation.
- The coding procedure should be symmetric or asymmetric (in the sense of the public key cryptographic algorithms), according to the application.
- Robustness against attacks, which use multiple watermarked copies, also known as collusion attacks.

General properties

- The algorithm should allow real-time processing [4].
- The algorithm must be adjustable to different degrees of robustness, quality and different amount of data.
- The algorithm should be tunable to different media [5].
- The algorithm should support multiple watermarks ([9], [4]).

3. AUDIO WATERMARKING AND APPLICATIONS

Copyright protection The copyright owner will be authenticated by the knowledge of the secret key to read the secret watermark.

Monitoring Embedding a secret watermark to enable the tracing of illegal copying [4].

Fingerprinting In point-to-point distribution environements information about authenticated customers can be embedded as secret watermarks right before the secure delivery of the data.

Indication of content manipulation The indication of content manipulation (tamper-proofing) from the authorized state could be detected by means of a public or fragile watermark.

Information carrier A public watermark embedded into the data stream can act as a link to external databases storing information about the copyright and license conditions.

4. THE WATERMARKING METHOD

The large amount of data of a typical audio signal in CD quality (178 kbyte) offers the possibility of using statistical methods relying on large sets.

The method presented below is a statistical algorithm working in the fourier domain. It embeds a 1-bit watermark in every time slice of about 1.2 seconds and doesn't nead the original audio stream or additional data to read the watermark.

The algorithms were motivated by the Patchwork approach [2]. Similiar methods are working in the time domain [1]. Our audio watermarking method has been adapted to the frequency domain and does not require the original in order to detect the watermark in contrast to other approaches [3, 5].

Let us assume a dataset containing $2N$ values (in our method frequency coefficients of the Fourier domain).

Embedding the watermark

1. Map the secret key and the watermark to the seed of a random number generator. Start the generator in order to pseudorandomly select two intermixed subsets $\mathcal{A} = \{a_i\}_{i=1,\dots,M}$ and $\mathcal{B} = \{b_i\}_{i=1,\dots,M}$ of equal size $M \leq N$ from the original set. [1]
2. Formulate the *test hypothesis* (H_0) and *alternative hypothesis* (H_1). The appropiate test statistic z will be a function of vectors $\vec{a}$ and $\vec{b}$ [2] with the pdf $\phi(z)$ in the unmarked and $\phi_m(z)$ in the marked case:
   H_0: The watermark is **not** embedded (z follows pdf $\phi(z)$).
   H_1: The watermark **is** embedded (z follows pdf $\phi_m(z)$).
   The two kinds of errors are incorporated in hypothesis testing:

$$\text{I:} \int_T^{+\infty} \phi(z)dz = P_I \qquad \text{(Type I error)} \tag{1}$$

$$\text{II:} \int_{-\infty}^{T} \phi_m(z)dz = P_{II} \qquad \text{(Type II error)} \tag{2}$$

3. Define P_I and calculate threshold T from equation (1).
4. Calculate the vector of parameters $\vec{k} \in \mathcal{K} = \{k_i\}_{i=1,\dots,2N}$, for a given P_{II}, T and embedding functions $e_{\mathcal{A}}, e_{\mathcal{B}}$:

$$\int_{-\infty}^{T} \phi_m(f(e_{\mathcal{A}}(\vec{a},\vec{b},\vec{k}), e_{\mathcal{B}}(\vec{a},\vec{b},\vec{k})))dz = P_{II} \tag{3}$$

5. Alter the selected elements $a_i \in \mathcal{A}$ and $b_i \in \mathcal{B}, i = 1,\dots,M$ according to the embedding functions $e_{\mathcal{A}}, e_{\mathcal{B}}$:

$$a_i' = e_{\mathcal{A}}(\vec{a},\vec{b},\vec{k}), b_i' = e_{\mathcal{B}}(\vec{a},\vec{b},\vec{k}), i = 1,\dots,M \tag{4}$$

   Besides the desired error probabilities the changes have to be distributed in a way, which achieves also the inaudibility.

[1] We define $\vec{a}$ and $\vec{b}$ as vector of elements from $\mathcal{A}$ or $\mathcal{B}$.

[2] $z = f(\vec{a},\vec{b})$ original and $z = f(\vec{a}',\vec{b}')$ marked data.

Detection

1. Map the secret key and watermark to the seed of the random number generator in order to generate the subsets $\mathcal{A}$ and $\mathcal{B}$.
2. Decide for the probability of correct rejection $1 - P_I$ according to the application and calculate the threshold T from equation (1).
3. Calculate the sample mean $E(z) = E(f(\vec{a}',\vec{b}'))$ and decide between the two mutually exclusive propositions:

$$H_0 : E(z) \leq T \quad \text{watermark is } \textbf{not} \text{ embedded} \tag{5}$$

$$H_1 : E(z) > T \quad \text{watermark } \textbf{is} \text{ embedded} \tag{6}$$

In subsequent sections we will investigate different test statistics and their applicability to the watermarking problem.

The embedding function The embedding functions should introduce changes, which are robust against differences in scale:

$$e_{\mathcal{A}} = (1+k)a_i, \quad e_{\mathcal{B}} = (1-k)b_i \tag{7}$$

$$a_i' = (1+k)a_i, \quad b_i' = (1-k)b_i, \quad i = 1,\dots,M \tag{8}$$

4.1. Test statistic I

The natural choice for the test statistic is the difference between the population means of $\mathcal{A}$ and $\mathcal{B}$ rather than their values per se. The standardized test statistic is given by :

$$z = f(\vec{a}',\vec{b}') = \frac{\bar{a}' - \bar{b}'}{\sigma_{\bar{a}'-\bar{b}'}} \tag{9}$$

Both sample means can be assumed normally distributed under the Central Limit Theorem, because of the large amount ($M \gg 30$) of Fourier coefficients. Therefore $\bar{a}' - \bar{b}'$ is normally distributed, and one can make the estimations $\sigma_{\bar{a}'} \approx \hat{\sigma}_{\bar{a}'}$, $\sigma_{\bar{b}'} \approx \hat{\sigma}_{\bar{b}'}$ and $\sigma^2_{\bar{a}'-\bar{b}'} \approx \hat{\sigma}^2_{\bar{a}'-\bar{b}'}$. The independence of the random variables $\bar{a}$ and $\bar{b}$, which are from the same set $\mathcal{A} \cup \mathcal{B}$ of Fourier coefficients, leads to the approximations $\bar{a} - \bar{b} \approx 0$.

Therefore we can formulate the two mutually exclusive propositions:

$$H_0 : \phi(z) = N(0,1) \tag{10}$$

$$H_1 : \phi_m(z) = N(\bar{z}_m, 1), \quad \bar{z}_m = \frac{k(\bar{a}+\bar{b})}{\hat{\sigma}_{\bar{a}'-\bar{b}'}} \tag{11}$$

with $N(\mu,\sigma^2)$ the normal distribution with mean μ and variance σ^2. With the equations (10) and (1) the threshold can be calculated as $T = z_{1-P_I}$. According to the symmetry of the normal distributions $\phi(z)$ and $\phi_m(z)$, k can be calculated from

$$\bar{z}_m - T = z_{1-P_{II}}. \tag{12}$$

An upper bound for k can be derived from the approximation

$$\hat{\sigma}^2_{\bar{a}'-\bar{b}'} \leq 2(1+k^2)\hat{\sigma}^2_{max} \qquad \hat{\sigma}^2_{max} := max(\hat{\sigma}^2_{\bar{a}}, \hat{\sigma}^2_{\bar{b}}) \tag{13}$$

This is a reasonable assumption because $\sigma_{\bar{a}}$ and $\sigma_{\bar{b}}$ are both estimators calculated from the mixed sets $\mathcal{A}$ and $\mathcal{B}$:

$$k \approx \frac{(z_{1-P_I} + z_{1-P_{II}})\varepsilon}{\sqrt{4 - (z_{1-P_I} + z_{1-P_{II}})^2\varepsilon^2}} \tag{14}$$

Therefore one can define the probabilities of correct detection $(1 - P_{II})$, rejection $(1 - P_I)$ measure the maximum relative error

$$\varepsilon := \frac{\sqrt{2}\hat{\sigma}_{max}}{\frac{\bar{a}+\bar{b}}{2}} \tag{15}$$

of the mean of set $\mathcal{A} \cup \mathcal{B}$ and calculate the necessary embedding factor k from equation (14). But a factor k ensuring the probabilites of correct detection or rejection according to equation (14) may result in audible distortions. To satisfiy both requirements one can define the probabilities of correct detection $(1-P_{II})$, rejection $(1 - P_I)$ use the embedding factor k according to subjective quality tests (see section below), and calculate the number of Fourier coefficients from (14).

4.2. Test statistic II

An extension of the test statistic according to (9) can be made by normalizing the random variable z from equation (9) to the mean $\frac{\bar{a}'+\bar{b}'}{2}$ of the whole set $\mathcal{A} \cup \mathcal{B}$:

$$z = f(\vec{a}', \vec{b}') = \frac{\frac{\bar{a}'-\bar{b}'}{\sigma_{\bar{a}'-\bar{b}'}}}{\frac{1}{2}\frac{\bar{a}'+\bar{b}'}{\sigma_{\bar{a}'+\bar{b}'}}} = 2\frac{\bar{a}' - \bar{b}'}{\bar{a}' + \bar{b}'} \tag{16}$$

Therefore according to equation (16) we expect z to be a random variable with mean 0 in the unmarked and an approximated mean of $\bar{z}_m \approx 2k$ in the marked case.

One disadvantage of this kind of test statistic in contrast to above the complicated pdf not suitable for the calculation of the threshold and embedding parameter. We measured $\bar{z}_m$ for different k and verified the linear relation of equation (16).

5. PROPERTIES OF THE ALGORITHM

5.1. Quality evaluation

The general approach in quality evaluation is to compare the original signal with the watermarked one for different k. To find the minimum embedding factor, with imperceptible or perceptible, but not annoying differences, between the reference and the watermarked signal, we used the so-called Subjective Diff-Grades (SDG) [7]: The selected 5 test items were excerpts of length 12s from the

SDG	Description
0.0	imperceptible
-1.0	perceptible, but not annoying
-2.0	slightly annoying
-3.0	annoying
-4.0	very annoying

Table 1: Subjective Diff-Grades used in listening tests

SQAM program material. The test pairs presented to the listener consist of the orginal and watermarked signal with different embedding factors k. The listener has to classify the difference in terms of the SDG scale. The result of the subjective quality evaluation were averaged over the number of listeners. The embedding factor $k = 0.10$ was used for the following robustness tests.

5.2. Security

The watermark and the marking procedure should also possess certain security properties. The space of distinguishable watermarks should be large enough, which is surely the case, because the number of different watermarks $N_W = \binom{2M}{M}$ for $M = 256$ results in approximately $4.7 \cdot 10^{152}$ watermarks. The probability of false detection of a watermark can be determined by performing the following steps:

1. Determine the number of bits B out of the M bits of the embedded watermark, which gives a false detection.
2. Calculate the probability that $i = B, \ldots, M$ bits match with the embedded bitpattern from:

$$\sum_{i=B}^{M} \frac{\binom{M}{B}\binom{M}{M-B}}{\binom{2M}{M}} \tag{17}$$

The threshold T indicating detection of the watermark were chosen to be half the size of the maximum value z for the embedded watermark. The thresholds are plotted as horizontal lines (Fig. (1)). We used different audio tracks and marked all the tracks

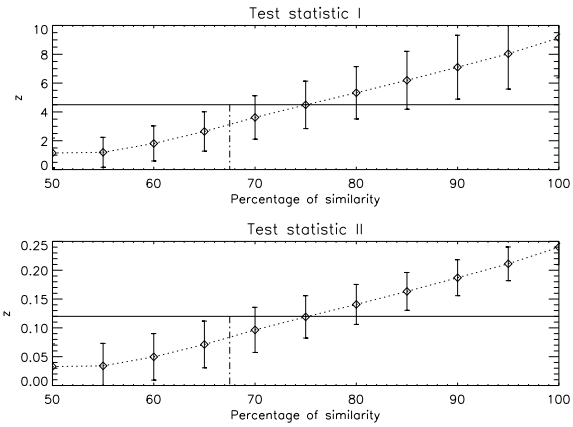

Figure 1: Security evaluation about the faked watermarks

with the same watermark and an embedding factor of $k = 0.15$. Afterwards we constructed 30 different bit patterns with a certain percentage of identical to the original pattern and measured the values for the random variables. For both cases we receive a critical similarity of about 67% with the original watermark.

According to equation (17), the probability of detecting a watermark which isn't embedded is $\leq 10^{-35}$ for statistic I.

5.3. Robustness

To test the robustness of the presented watermarking algorithm we randomly choose 400 different combinations of watermarks and keys and embedded this bit pattern 10 times into one audio track. All files were 16-bits signed stereo sampled at 44.1 kHz (CD quality).

Test conditions All audio signals were watermarked with a embedding factor of $k = 0.10$ and subsequently manipulated (Fig. (2)).

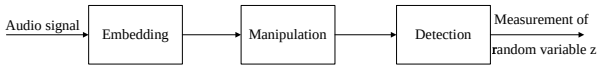

Figure 2: Test scenario to measure detection values z

To measure the robustness the total error probability $P_{error} = P_I + P_{II}$ due to the overlap of the pdf's in the unmarked and marked case were calculated from equations (1-2).

MPEG 1 Layer III audio compression The robustness against MPEG 1 audio Layer III compression has been tested by using a compression rate of 128 kbps for the watermarked signal.

Filtering To test the robustness against filtering a bandpass filter was applied to the watermarked signal by amplifying the signal by -9 dB in the low and high frequency domain. The cut-off frequencies has been 441 Hz for the low-pass and 4410 Hz for the high-pass filter.

Resampling The original audio signals were sampled with a sampling rate of 44.1 kHz. The sampling rate of the watermarked audio data was reduced to 22,05 kHz and resampled to the original rate of 44,1 kHz. This causes audible distortions especially in audio tracks carrying high frequencies.

Requantization Audio tracks sampled at 8-bit are often used in games and multimedia applications. We therefore tested the process of requantization of a 16-bit watermarked audio signal to 8-bit and back to 16-bit. This increases the incoherent background noise of the audio track due to the rounding errors during the processing.

Robustness against cropping The embedding of the watermark in every time slice of about 1.2 seconds enables the detection of the watermark even in the case of cropping or cutting, provided we have a contiguous part of at least about 2.5 seconds from the watermarked audio stream.

Test results

	MPEG	Filtering	Resampling	Requantisation
Error/%	1.22	1.47	1.29	1.43

Table 2: Total error probabilities for different manipulations

The error probabilities of the several manipulation of the watermarked signal can be easily reduced by using more frequency coefficients. This is equivalent to the embedding to the watermark in a longer time slice.

6. POSSIBLE ENHANCEMENTS OF THE ALGORITHM

The watermarking algorithm presented leaves room for further research in a variety of ways. Other test statistics and embedding functions can be investigated. To ensure the quality of the material a psychoacoustic model controlling the embedding procedure should be integrated. The embedding of multiple non-interfering watermarks into the same audio track is demanded by certain applications. Furthermore one of the greatest challenges is the robustness against the so-called jitter attack [8].

7. CONCLUSION

In this paper the watermarking of audio with respect to different kinds of watermarks were presented and possible applications discussed. The algorithm presented is a statistical approach working in the Fourier domain. The application of different test statistics in the algorithm were investigated. The watermarking techniques were evaluated in terms of quality, security and robustness. The security is guaranteed by the huge number of watermarks and the vanishing probability of faking a watermark. The algorithm shows good robustness against common signal processing. Possible enhancements were discussed and are subject of current research.

8. ACKNOWLEDGMENT

This work was partially founded by WEDELMUSIC (Web DELivering of Music scores) (http://www.dsi.unifi.it/wedelmusic/), a Research and Development project in the IST programme of the European Commission.

9. REFERENCES

[1] P. Bassia and I. Pitas, *Robust audio watermarking in the time domain*, Signal processing IX, theories and applications: proceedings of Eusipco-98, Ninth European Signal Processing Conference, Rhodes, Greece, 8–11 September 1998 (Patras, Greece) (S. Theodoridis et al., eds.), Typorama Editions, 1998, pp. 25–28.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, *Techniques for data hiding*, IBM Systems Journal **35** (1996), no. 3&4, 313–336.

[3] Laurence Boney, Ahmed H. Tewfik, and Khaled N. Hamdy, *Digital watermarks for audio signals*, 1996 IEEE Int. Conf. on Multimedia Computing and Systems (Hiroshima, Japan), 1996, pp. 473–480.

[4] Christoph Busch, Wolfgang Funk, and Stephen Wolthusen, *Digital watermarking: From concepts to real-time video applications*, IEEE Computer Graphics and Applications **19** (1999), no. 1, 25–35.

[5] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon, *Secure spread spectrum watermarking for multimedia*, Technical Report 95-10, NEC Research Institute, 1995.

[6] Kerckhoffs, A., *La cryptographie militaire*, Journal des Sciences Militaire **9th series** (1883), 161–191.

[7] C. Neubauer and J. Herre, *Digital watermarking and its influence on audio quality*, Proceedings of the 105th Convention of the Audio Engineering Society, San Francisco, USA 26–29 September, 1998 (Anonymous, ed.), 1998.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Attacks on copyright marking systems*, Second International Workshop on Information Hiding, 14–17 April, 1998, Portland, Oregon, USA (Berlin, Germany / Heidelberg, Germany / London, UK / etc.) (David Aucsmith, ed.), Lecture Notes in Computer Science, vol. 1525, Springer-Verlag, 1998, pp. 219–239.

[9] L. Piron, M. Arnold, M. Kutter, W. Funk, M. Boucqueau, and F. Craven, *Octalis benchmarking: comparison of four watermarking techniques*, Security and Watermarking of Multimedia Contents (San Jose, California) (Ping Wah Wong and Edward J. Delp, eds.), vol. 3657, January 1999, pp. 240–250.