Audio Binary Halftone Watermarking Algorithm

Huan Li a, b, a*, Zheng Qin a, Xuanping Zhang a, Xu Wang a

a School of Electronics and Information Engineering, Xi’an Jiaotong University, Shanxi, China
b Department of Computer Science, Dongguan University of Technology, Guangdong, China

Abstract

Conventional audio watermarking method has the following deficiencies: the embedded watermarking signal bits are too less; the image watermarking pre-process is too simple which reduce the security; the embedded audio watermarking is meaningless binary sequence. To address these problems, we propose a robust audio watermarking algorithm based on audio binary halftone pre-process. The meaningful audio watermarking can be preprocessed to high-fidelity binary audio. The variable dimension operation is used to scramble the host audio. Experiments show the proposed algorithm has big embedding quantity, high security, strong practicability and robustness in enduring common attacks.

© 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and/or peer-review under responsibility of [CEIS 2011]

Keywords: Robust Audio Watermarking; Audio Binary Halftone; Variable Dimension

1. Introduction

With the development of computer and network technology, people gradually go into the network and the information age. More and more information resources can be accessed through wired and wireless network, but information security and protection of property rights problem become obviously [1, 2]. In recent years, many digital watermarking algorithms have been proposed for intellectual property right protection of digital media data [3, 4]. In this paper, audio binary halftone watermarking algorithm is proposed. Comparing with the conventional audio watermarking methods, the proposed algorithm has the following advantages: 1) the watermarking signal bits are embedded more; 2) unlike the image watermarking, the audio watermarking is embedded; 3) the audio watermarking is meaningful binary sequence. The proposed algorithm has big embedding quantity, high security, strong practicability and robustness in enduring common attacks.

* Corresponding author. Tel.:0086-0769-22861226;
E-mail address: lihuan@dgut.edu.cn.
2. The Related Definitions

2.1. The Variable Dimension Operation

The objective of variable dimension operation is to change the dimension of audio sequence, and then use the arbitrary high dimention matrix to scramble it.

Definition 1: dimension increasing
Let \( L \) denote the audio sequence length, \( x \) denote the audio position coordinate, \( x \in [1, L] \). In order to get an \( n \)-dimensional audio coordinate \((x_n, x_{n-1}, \ldots, x_1) \in m^n\), the dimension increasing operation is defined in Eq.1, where \( m \) satisfies \((m-1)^n < L \leq m^n\), the symbol ‘/’ denotes the integer division operation.

\[
x_i = (x / m^{-1}) \mod m \quad (i = 1, \ldots, n)
\] (1)

Definition 2: dimension decreasing
Let \( L \) denote the audio sequence length, \((x_n, x_{n-1}, \ldots, x_1)\) denote the \( n \)-dimensional audio coordinate. In order to get the one-dimensional audio coordinate \( x \), the dimension decreasing operation is defined in Eq.2, where \( m \) satisfies \((m-1)^n < L \leq m^n\).

\[
x = \sum_{i=1}^{n} x_i \cdot m^{-i} \quad (i \in [1, n])
\] (2)

3. Pre-process Algorithm

3.1. Audio watermarking Binary Halftone Pre-process

According to early work about audio binary halftone [5], meaningful digital audio watermarking is processed to high-fidelity binary audio. Based on Floyd error diffusion algorithm [8], we proposed an Audio Binary Halftone process algorithm. In our method, the error which is caused by waveform conversion from sine wave to a square wave is feedback to follow-up audio sequence. This method is called digital audio binary halftone procedure. The error diffusion model is given in Fig.1, where, \( m(x) \), \( n(x) \), \( p(x) \), and \( e(x) \) respectively denote input data, output data, input data by preceding step error diffusion, quantization error, \( Q(.) \) is threshold quantization, and \( W(k) \) is Floyd-Steinberg error diffusion filter.

The related computer formulas are as follows:

\[
p(x) = m(x) + \sum_k w(k) \cdot e(x - k)
\] (3)

\[
n(x) = Q(p(x)) = Q(m(x) + \sum_k w(k) \cdot e(x - k))
\] (4)

\[
e(x) = n(x) - p(x)
\] (5)

The value of \( Q(.) \) is selected by practical situation, and the parameters of \( W(k) \) are: \( W(1)=7/16 \), \( W(2)=5/16 \), \( W(3)=3/16 \), \( W(4)=1/16 \). So the meaningful audio watermarking is transferred to one-dimensional binary sequence, from which we can clearly listen the information of original audio.

![Fig. 1. The error diffusion model](image-url)
3.2. Host Audio signal pre-process

For host audio, we use variable dimension operation to change the dimension of coordinates and uses arbitrary high-dimensional matrices to scramble the audio. The Host Audio signals pre-process is showed as follows.

Input: The host audio signals: \( Y \), length of \( Y \): \( L \), dimension variable: \( n \)

Output: The new scrambled audio signals: \( Y' \)

Procedure:
1. Step1: compute \( m \) according to \((m-1)n < L \leq mn\);
2. Step2: supplement ‘0’ to audio sequence \( Y \), the number of ‘0’ is \( h = mn - L \), so the length of audio sequence \( Y \) becomes \( L + h = mn \);
3. Step3: generate a random \( n \)-dimensional arbitrary matrix \( A_{n \times n} \) according to the method in [6];
4. Step4: initialize a new audio sequence \( Y' \) with the length is \( mn \);
5. Step5: for \( x = 1 \) to \( L \), do
   1). according to dimension increasing operation (Eq.1), to get an \( n \)-dimensional audio coordinate \( (x_n, x_{n-1}, \ldots, x_1) \);
   2). for \( n \)-dimensional audio coordinate \( (x_n, x_{n-1}, \ldots, x_1) \), use the high dimensional matrix transformation to map \( (x_n, x_{n-1}, \ldots, x_1) \) to \( (x'_n, x'_{n-1}, \ldots, x'_1) \), with the generated transform matrix \( A_{n \times n} \) in Step3;
   3). for any \( (x'_n, x'_{n-1}, \ldots, x'_1) \), use dimension decreasing operation (Eq.2) to get the mapped one-dimensional audio coordinate \( x' \);
   4). the new scrambled audio signals value \( Y'(x') \) is assign by \( Y(x) \).

4. The Realization of Algorithm

In this section, we give the watermarking embedding scheme, extraction scheme, and the realization procedure of algorithm.

4.1. Watermarking Embedding Scheme

The pre-processed \( 1 \)-dimensional binary audio watermarking is embedded in the average statistical of pre-processed host audio signals sampling value.

Let \( L \) denote the pre-processed host audio signals length, which was divided to \( K \) segments, and each segment has \( R \) audio sample points. Let \( T \) denote the pre-processed \( 1 \)-dimensional binary audio watermarking and \( B(i) \in [0, 1] \), \( 1 \leq i \leq K \) ; Let \( A(j) \) denote the audio point in \( i \) segment, \( A'(j) \) denote the embedded sample point, and \( S \) is the max of the values that satisfy the Eq.6:

\[
A'_j = \begin{cases} 
A(j) - A(j) \mod S + 3S / 4, & \text{if } B(i) = 1; \\
A(j) - A(j) \mod S + S / 4, & \text{if } B(i) = 0;
\end{cases}
\]

4.2. Watermarking Extraction Scheme

According to the idea of maximum likelihood decoding, we extract the watermark. Let \( B'(s) \) denote the extracted watermark, \( \rho(B', B) \) denote the correlation function:

\[
\rho(B', B) = \sum_{i=1}^{T} B'(i), B(i)
\]

If exits \( \rho(B', B) \geq T \), \( T \) denote threshold, we think the watermark is extracted.
4.3. The Realization Procedure of Algorithm

Based on above contents in this paper, we proposed a robust audio watermarking algorithm based on audio binary halftone preprocess. The frame diagram of proposed algorithm is given in Fig.2. The algorithm includes two sub-procedures: Embedding sub-procedure and Extracting sub-procedure.

Fig.2. the frame diagram of the proposed algorithm

1) Embedding sub-procedure
   Step1: according to audio binary halftone pre-process, the meaningful audio watermarking is pre-processed to binary audio watermark;
   Step2: according to the host audio signal pre-process, the host audio is pre-processed to scrambled audio;
   Step3: according to the Eq.6, embed the binary audio watermark in the scrambled host audio sequence
   Step4: get the audio with watermark.

2) Extracting sub-procedure
   Step1: according to the host audio signals pre-process, the audio signals with watermarking (attacked or non-attacked) is processed to a scrambled audio.
   Step2: according to the Eq.7, extract the binary audio watermarking;
   Step3: test the performance of the extracted watermarking.

5. Experiment Results and Analysis

In this section, we give some experiments to testify the performance of the proposed algorithm. We use ‘start.wav’ as audio watermarking, and host audio signals sample ‘close.wav’. We selected 500 points of the ‘start.wav’ as Fig.3c. From the audio binary halftone pre-process experiment (Fig.3d), audio watermarking ‘start.wav’ is processed to high-fidelity binary audio.
Fig. 3. the wave plots of audio and binary halftone pre-process experiment

We randomly generated 1 group of arbitrary high dimensional transform matrices (Fig. 4a, 4b). The proposed algorithm has a wonderful one-time scrambling performance Fig. 4c. The scrambled audio with watermarking (Fig. 4d) has similar plot with the original host audio plot and it has good listening performance.

![Figure 4](attachment:image.png)

(a) $A_1, m=11$ (b) inverse matrix $A_1'$ (c) scrambled host audio (d) scrambled host audio with watermarking

Fig. 4. Host audio signal pre-process experiment

After some different attacks, such as zero-cross, Gaussian noise addition, data loss, data amplification and data reduction, etc, the algorithm has good robustness.

![Figure 5](attachment:image.png)

(a) extracted audio by zero-cross (b) extracted audio by Gauss noise (c) extracted audio by data loss $1/3$ (d) extracted audio by Mp3

Fig. 5. Extracted audio watermarking from host audio in different attacks

6. Summary

The proposed algorithm respectively pre-processed the audio watermarking and host audio in different methods, which increase the security. Experiments show that the proposed algorithm has a wonderful pre-process performance, high imperceptibility, and robustness in enduring common attacks.

7. References


