A public key audio watermarking using patchwork algorithm

Doo Gun Hong, Se Hyoung Park, and Jaeho Shin
Department of Electronic Engineering, Dongguk Universitiy, Seoul,100-715, Korea.
Tel. +82-2-2260-3336, Fax.: +82-2-2272-5667
e-mail : hong9eks@yahoo.co.kr

Abstract : This paper presents a statistical technique for audio watermarking. We describe the application of the promising public key watermarking method to the patchwork algorithm. Its detection process does not need the original content nor the secret key used in the embedding process. Special attention is given to statistical method working in the frequency domain. We will present a solution of robust watermarking of audio data. In this scheme, an extension of patchwork audio watermarking is presented which enables public detection of the watermark.
Experimental results show good robustness of the approach against MP3 compression and other common signal processing manipulations.

1. Introduction

Recently a need has arisen for protecting the copyright ownership of electronic media, such as image, video and audio data. Digital signal processing technologies have also made it easy to unlawful copy, modify and redistribute multi-media data without regard for copyright own-ership. The one of promising copyright protection mechanisms is digital watermarking of multim-edia data, because it allows the owner to embed side information into the host data without a defect. Even though watermarking is not an effective copyright enforcement technology, it is believed to be a good deterrent from unlawful copying and dissemination of copyrighted audio [3][5]. When the copyright violation has occurred, watermark can provide evidence of copyright infringements. Many watermarking algorithms are now available and most of them are applicable to image or video data.

However, audio watermarking algorithms are hardly researched. There are several reasons why to develop audio watermarking algorithms are not easy. Firstly, the human ear is far more sensitive than other human sensory organs like eyes. Human ears can detect even a small amount of embedded noise. Secondly, audio clips are rather short compared with video clips in terms of time and file size[1][7][11]. Thus, information that is hidden on audio clips is to be much relatively higher noise component than image or video. Consequently, it tends to degrade the quality of audio but an intentional noise inserted into the digital audio clip to identify the copyright information such as author, recording label, and usage rules.

Audio watermarking algorithms must satisfy at least two constraints. The first constraint is not to degrade audio quality. Embedded audio watermarks should be almost inaudible. Then, the embeded noise should be almost imperceptible. The second constraint is robustness. The algorithm should be robust enough to withstand attempts such as removal or alteration of inserted waterma-rks. These two constraints may seem to be contradictory. However, they must be satisfied it.[1][2][3]

Most of watermark algorithms are using random generator for generating watermarking sequence or randomly choosing audio samples. It is need to use secret key. These methods are similar to symmetric encryption like DES. In practical application symmetric schemes lead to a security problem if the detection are implemented in consumer devices that are spread all over the world, the detector reveal a secret key on purpose. Therefore, the development asymmetric schemes are inevitable. In such a asymmetric scheme the detector only needs to know a public key, which does not give enough information to remove or make watermark. In this paper we propose a public key watermarking scheme to the patchw-ork algorithms.

The Patchwork algorithm was proposed for image watermarking by Bender[1]. In the patchwork algorithm, a secret key is used to initialize a pseudo-random number generator, which outputs the locations of the cover, which will host the watermarking[1]. Patchwork invisibly embeds in a host image with a specific statistic, one that has a Gaussian distribution. This unique statistic indicates the presence or absence of a signature[1][3][7]. So we modify patchwork algorithm for audio watermarking and to be an asymmetric scheme.

The rest of this paper is organized as follows. Section 2 introduces patchwork algorithms of digital audio watermarking. We propose a public key watermarking scheme in Section 3. The empirical tests of the proposed watermarking technique are presented and discussed in Sections 4 and 5. Finally, Section 6 concludes conclusion this paper.

2. Patchwork Algorithm of digital audio watermarking

The step of the patchwork algorithm can be summarized as follows[1].

In the embedding process, the owner selects n-pixel pairs pseudorandom according to a secret key k and then modifies the luminance values (a, b) of the n pairs of pixels by using the following formula:

$$\tilde{a}_i = a_i + \delta \qquad \text{(1)}$$
$$\tilde{b}_i = b_i - \delta$$

Thus, the owner simply adds □ to all values a and subtracts □ from every b. In the detection process, the n-pixel pairs that were used in the embedding step to host the watermarking are retrieved, again using the secret key k. Then, the sum

$$S = \sum_{i=1}^{n} \tilde{a}_i - \tilde{b}_i \qquad \text{(2)}$$

is computed. If the cover actually contained a watermarking, we can expect the sum to be $2\delta n$, otherwise it should be approximately zero. The detection is based on the statistical assumption

$$E[S_n] = \sum_{i=1}^{n} E[a_i] - E[b_i] = 0 \qquad \text{(3)}$$

If we randomly choose several pairs of pixels in an image and assume that they are independent and identically distributed. As a consequence, only the owner, who knows the modified locations, can obtain a score close to

$$S = \sum_{i=1}^{n} \{(a_i + \delta) - (b_i - \delta)\} = 2\delta n + \sum_{i=1}^{n} (a_i - b_i) \qquad \text{(4)}$$

So each step of the way we accumulate an expectation of $2\delta n$.

As n or δ increases, the distribution of shifts over to the right like figure 1.

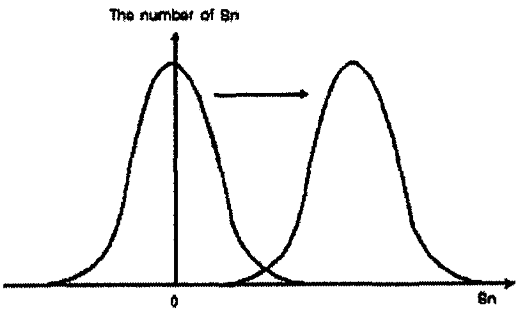

Fig. 1. Shift of expectation.

If we shift it far enough, any point that is likely to fall into one distribution is highly unlikely to be near the center of the other distribution. Since its first appearance, some extensions of this algorithm have been proposed in order to hide a message longer than one bit and increase the robustness of the scheme[1].

3. Embedding the Watermarking

The proposed algorithm inserts watermarks in the frequency domain. Assume that N bits of copyright information be embedded into secret key and public key respectively. Let n be the number of embedded samples.

Embedding steps are summarized as follows:

Map the secret key and public key the watermark to the seed of a random number generator. Next, generate two index set of secret key $I^s = \{I_1, \ldots I_n$ whose elements are pseudo-randomly selected integer values from $I \le 10000$. And then generate two index set of public key, $I^p = \{I_1, \ldots I_n$ whose elements are chosen same as secret key index.

Note that two index sets, I^s and I^p, are needed to denote secret key index set and public key index set, respectively. Distinct multiple index sets can also be used to designate multiple-watermark information in one bit code.

Then We select discrete cosine transform coefficients from cover audio data with block length 1024. So DCT coefficients set F are composed. This step is repeated until the number of set elements are to be 10000.

Define $a = \{a_1, \ldots, a_n\}$ as the subset of F whose subscript corresponds to n elements of the index set. Similarly, define as follow :

$$\begin{aligned} a &= \{a_1, \ldots, a_n\} \\ b &= \{b_1, \ldots, b_n\} \\ c &= \{c_1, \ldots, c_n\} \\ d &= \{d_1, \ldots, d_n\} \end{aligned} \qquad \text{(5)}$$

The embedding functions should introduce change, which are robust against differences in scale

$$\begin{aligned} &a_i' = a_i + k_1\delta, \quad b_i' = b_i - k_1\delta \quad i = 1, \ldots, N \\ &c_i' = c_i + k_2(a_i' - b_i'), \quad d_i' = d_i - k_2(a_i' - b') \end{aligned} \qquad \text{(6)}$$

Finally, replace the selected elements

a_i, b_i, c_i and d_i by a_i', b_i', c_i' and d_i'

In embedding process we select $\delta = \sigma_{a'-b'}$.

4. Test statistic and Detection

We choose the test statistic for secrete key

$$z = f(a_i',b_i') = \frac{a_i' - b_i'}{\sigma_{a_i'-b_i'}} \quad (7)$$

Both sample means can be assumed normally distributed under the Central Limit Theorem, because of the large amount($n = 100 >> 30$) of DCT coefficients.

Secret key hypothesis :

$$H_{s0} : \phi(z) = N(0,1)$$

$$H_{s1} : \phi_m(z) = N(\bar{z}_m,1), \quad \bar{z}_m = \frac{2k_1\delta}{\sigma_{a_i-b_i'}} \quad (8)$$

But we select $\delta = \sigma_{a'-b'}$, and embed n times. So mean of test statistic z is

$$\bar{z}_m = 2\sqrt{n}k_1 \quad (9)$$

Type I error and type II error are calculated by threshold T_1. This test statistics are following gaussian distribution, so we can determine threshold. Then we can compute k_1. If the watermarked audio has audible noise with computed k_1, we can control the noise with changing embedded sample n, but it is reduce bitrates of watermark.

Now we choose the test statistic for public key. In public key also take test statistic same as secret case. But we choose other method.
First linear transformation with two public key index set

$$Y_1 = c_i' - d_i'$$

$$Y_2 = c_i' + d_i' \quad (10)$$

these new variables Y_1, Y_2 also has to be statistic variables with same distribution.
And we make new test statistic

$$O = \frac{\sigma_{Y1}^2}{\sigma_{Y2}^2} \quad (11)$$

where O has F-distribution with freedom degree $(n-1, n-1)$.
To detect public watermark we calculate variance $\sigma^2 = E(c_i' \pm d_i')^2$ and to decide watermarked or not watermarked.

Not watermarked case :

$$v_0 = \frac{\sigma^2{}_{Y_1}}{\sigma^2{}_{Y_2}} = \frac{E(c_i - d_i)^2}{E(c_i + d_i)^2} = 1 \quad (12)$$

Watermarked case :

$$v_0 = \frac{\sigma^2{}_{Y_1}}{\sigma^2{}_{Y_2}} = \frac{E(c_i - d_i)^2}{E(c_i + d_i)^2}$$

$$= \frac{2\sigma^2 + 4k_2{}^2(2\sigma^2 + 4k_1{}^2\delta^2)}{2\sigma^2} \quad (13)$$

$$= 1 + 4k_2{}^2(1 + 2k_1{}^2)$$

And public key hypothesis :

$H_{p0} : v_0 \le T_2$ Watermark is not embedded

$H_{p1} : v_0 > T_2$ Watermark is embedded

5. Robustness Test

To test the robustness of the presented watermarking algorithm we randomly choose 10000 random number for each index set whose elements of DCT set F Different combinations of watermarks and keys and embedded this bit pattern 5 times into one audio track. All files were 16-bits signed stereo sampled at 44.1kHz. The audio samples include Rock, Jazz and Classical music The location-shift change parameter $T_1 = 4$ and the threshold $T_2 = 1.36$ were adopted. To test the robustness of the algorithm against various types of manipulations, the following signal processes were employed.

1. MPEG1 Layer□ audio compression : The robustness against MPEG1 audio Layer□ compression has been tested by using a compression rate of 128kbps for the watermarked signal.
2. Resampling : The original audio signals were sampled with a sampling rate of 44.1kHz. The sampling rate of the watermarked audio data was reduced to 22.05kHz and resampled to the original rate of 44.1kHz. This causes audible distortions especially in audio tracks carrying high frequencies.
3. Echo addition : In the detection function only echo echo delays between 0.5 and 3 milliseconds are considered. Below 0.5ms the function does not work properly and above 3ms the echo becomes too audible.

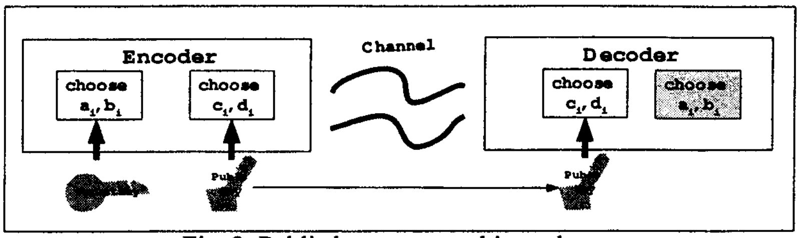

Fig. 2. Public key watermarking scheme

Table 1. Test result(pop song Max8 album1 18 samples)

	Error bits / Total inserted bits (18 samples, 1 min)	Bit Error Rate
Echo	3/450	0.667%
Mp3	3/450	0.667%
Filter	10/450	2.222%

6. Conclusion

In this paper presented a new public key watermarking based on statistic method. It is possible to detect watermark with the public key. Since the public key is open to the public, the detection is called the public detection. Simple analysis shows how robust to attack and the watermark is not feasible. Those who do not have the knowledge of the secret key cannot remove the watermark. But attacker is focused on obscuring public detection, it is still possible detection by the public key if the system is properly designed.

Acknowledgements
This research waw supported byBrain Korea 21 Program of Korea Research Foundation.

References

[1] W. Bender, D. Gruhl, Morimoto and A. Lu, "Techniques for Data Hiding," IBM Systems Journal, vol. 38, no.3&4, pp. 313 - 336, 1996.

[2] J.J. Eggers, J. K. Su, and B. Girod, "Public key watermarking by eigenvectors of linear transforms", In Proc. Of European Signal Processing Conf., Tampere, Finland, April 2000.

[3] M. Arnold, "Audio watermarking: features, applications and algorithms," Multimedia and Expo, 2000. IEEE International Conference, vol. 2, pp. 1013-1016, 2000.

[4] Kii. H, Onishi. J, Ozawa. S, "The digital watermarking method by using both patchwork and DCT," Multimedia Computing and Systems, 1999. IEEE International Conference on vol. 1, pp. 895-899, 1999.

[5] I. J. Cox, J. Killian, T. Leighton and T. Shamoon, "Secure Spread Spectrum watermarking for Multimedia," NEC Research Institute, Technical Report 95-10, Oct. 1995.

[6] In-Kwon Yeo, Hyoung Joong Kim, "Modified Patchwork Algorithm: a novel audio watermarking scheme," Information Technology: Coding and Computing, 2001 Proceedings International Conference on, pp. 237-242, 2001.

[7] Steven M. Kay, "Fundamentals of Statistical Signal Processing Volume□: Detection Theory," Prentice Hall, 1998.

[8] R. G. van Schyndel, A. Z. Tirkel, and I. D. Svalbe, "Key independent watermark detection", In Proc. Of the IEEE Intl. Conf. on Multimedia Computing and Systems, vol. 1, Florence, Italy, June 1999.

[9] S. Katzenbeisser and Fabien A. P. Petitcolas, "Information Hiding," Artech House Publishers, 2000.

[10] 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), pp. 473-480, 1996.

[11] C. Neubauer and J. Herre, "Digital watermarking and its influence on audio quality," Proceedings of the 105th Convention of the Audio Engineering Society, SanFrancisco, USA 26-29 September, 1998.

[12] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," Proceedings of the IEEE, vol. 86, pp. 1064-1087, 1998.

[13] ISO/IEC 11172 part 3: audio, first edition, August, 1993.

[14] SDMI, Call for Proposals for Phase □ Screening Technology, Version 1.0, 1999.