# A Robust Digital Watermarking System Adopting 2D Barcode against Digital Piracy on P2P Network

*Eui-Hyun Jung*[†] *and Seong-Yun Cho*[†]*,*

[†]Dept. of Digital Media, Anyang University, Korea

**Summary**
Due to the proliferation of the P2P network, digital content can be easily shared without any restriction, and P2P network permits a great amount of digital piracy. Though a lot of DRM architectures have been announced, those can not show any effective method against digital piracy on P2P community. To resolve the point issues, a novel robust digital audio watermarking scheme is presented to support insertion of dynamically generated user data into the digital content on the side of digital content provider. Embedding of watermarks is performed using 2D barcode in wavelet domain. The 2D barcode is insensitive to noise and has embedded error correction facility. In the proposed system, digital content consumer's information is signed and encrypted whenever the consumers initiate download of audio data. This information is dynamically encoded into 2D barcode as a watermark to the audio data. From the experimental result, the proposed system shows better inaudibility and robustness comparing with the conventional methods.

***Key words:***
*Digital Piracy, Watermarking, P2P*

## Introduction

As an effective digital distribution media, the Internet makes new media environment. From this basis, digital contents, music, images, video, books and games, can be directly distributed from digital content providers to end-users. This situation shows new business opportunities to digital content publishing industry and enables end-users to enjoy convenient digital environment. On the other hand, widespread unauthorized distribution and illegal reuse of digital contents through the Internet have caused a large amount of revenue loss of digital content providers. To protect digital assets and manage their distribution on the Internet, researchers and IT industry invest their time and efforts to suggest various systems such as WMRM [1], Rights|System [2] and EMMS [3], which are commonly called as Digital Rights Management (DRM).

DRM is a collection of a technology and related systems including key management system, media distributor, and custom viewer that protect the copyright of digital content providers and prevent unauthorized usage [4]. Although DRM can provide a well-structured system for protecting digital content efficiently, it has unavoidable problem of interoperability because most DRM vendors suggest proprietary plug-in, viewers and file extension for their purpose. From this reason, the watermarking is a simple and an effective approach for protecting the copyright [5].

Watermarking is a pattern of bits inserted into a digital image, audio or video file to identify the file's copyright information. The purpose of digital watermarks is to bind copyright information such as content owners to intellectual property that's in digital format [5]. Unlike printed watermarks, which are intended to be somewhat visible, digital watermarks are designed to be completely invisible or inaudible, in the case of audio clips. Although an unauthorized content usage can not be prohibited using watermarking, it can be used to trace the digital pirates forensically. Since watermarked content can be detected on the Internet using web spiders, the copyright violation can be notified easily and the infringer will be likely taken to court.

Unlike image files on the Web server, audio files are mainly distributed on the P2P community. In this situation, a simple watermark containing only copyright information can not catch digital pirates because there is no information who is the originator of illegal distribution. To extract the information of the owner from illegally shared content on the P2P, digital content distributors should have ability to make watermark dynamically according to distribution information such as consumer's IP and download time.

In the early stage, there are some researches on audio watermarking placing such as higher frequency region [6] or using Fourier transform phase coefficients [7] or using echo signals [8]. However, existing researches have concentrated on how to hide or scatter static information to audio files. Moreover, the watermark in these researches is meaningless image that did not contain highly structured information such as digital signing. Though simple image is enough for watermark to assure copyright owner's information, the image can not provide proper consumer's information. To provide this information, the image should be an encoded form containing highly structured data. However, there is another issue in using encoded high structured image. Most of all, it is not avoidable for watermark to be distorted due to attacks or normal data manipulation such

Manuscript received October 5, 2006.
Manuscript revised October 25, 2006.

as compression. If watermark having highly structured data is distorted, it can not be used to restore to original information.

An audio watermarking scheme is proposed in this research that supports insertion of dynamically generated data into digital audio content using image data. Ordinary image data are vulnerable and will be large to hold digital sign or encrypted data, so 2D barcode [9] is adopted. In the proposed system, consumers' information is signed and encrypted whenever consumers initiate download of audio data. This information is dynamically encoded into 2D barcode as a watermark to the audio data. Embedding of watermark is performed in wavelet domain. Because 2D barcode is insensitive to noise and has self-error correction, the algorithm is robust to lossy compression such as MPEG-1 Layer III and down-sampling.

This paper is organized as follows. Requirements and design factors for watermarking suitable for P2P network are described in Section 2. In Section 3, the architecture of the audio watermarking embedding and detection is described. The evaluation results are presented in Section 4 and the conclusions are presented in Section 5.

## 2. Technological Issues of Watermarking Scheme for P2P Network

### 2.1 Requirements of Proper Watermarking for P2P Network

Although P2P networks are considered as a new computing paradigm, they have dark side of providing working place for digital pirates. From [10], about 80% of unauthorized distributed audio contents are on the P2P community. However, most DRM systems are designed as a closed system; they don’t give any concern to prohibit illegal sharing of digital audio content in P2P community. Comparing to DRM, watermarking over audio digital content can be a simple but effective method against illegal distribution on P2P networks.

However, simple digital watermark containing only owner’s copyright is not enough to protect illegal sharing on P2P networks. Unlike digital contents on Web sites, content providers can not trace who is the first distributor in P2P network because of its users’ anonymity. Nevertheless, existing watermarking researches have concentrated on how to hiding watermark in digital contents [11][12], not how to structure watermarking contents for application domains especially P2P networks. Generally, watermark system targeted for P2P networks should be designed to satisfy following requirements.

- Watermark should have consumer’s information

  Most watermarks presents owner’s copyright, but a watermark for P2P networks have consumers’ data to trace distributors. Therefore watermark should be generated on download time based on consumers’ data.

- Watermark should be robust to both legal or illegal digital manipulation

  Digital contents on P2P tend to be manipulated such as file format changing or re-sampling. These manipulations can cause modification of digital byte stream in original digital contents, which results to attack inserted watermark.

- Data in watermark is hard to modify by unauthorized users

  Since watermark contains critical data as forensic evidence, it must not be counterfeited or modified. It may be destroyed but it should not be changed to other data at least.

From the above considerations, watermark for P2P networks should be dynamically generated whenever consumers issue a download. In addition, it is not only encrypted, but also robust to the data manipulation. Unfortunately, these design considerations are somewhat contradictory. To protect consumer’s data modification, it should be encrypted or digital signed. However encrypted data tends to be very sensitive to noise, so encrypted data may not be used as a watermark in noisy environment.

### 2.2 Design Factors

Due to the conflicting requirements of watermark for P2P networks, data types of watermark should be examined. Data types of watermark can be text or raster image because watermarking does not be affected by contents of watermark. However, data types of watermark are highly related to information hiding and robustness. As shown in Table 1, data types used in watermark has pros and cons. Generally, plain text or image as a watermark is vulnerable to modification. Cipher text or image is robust to hacking, but one bit change corrupts original data completely.

Table 1: Comparison of data types to be used in Watermark

| | Plain Text | Cipher Text | Plain Image | Cipher Image |
|---|---|---|---|---|
| Attack | Weak | Strong | Weak | Strong |
| Noise | Weak | Very Weak | Strong | Weak |

As described above section, it is desirable for watermark to be both encrypted and strong to noise. From these requirements, cipher image is superior candidate to other data types, but it also has weakness to noise. To resolve this confliction, 2D barcode image is adopted in this paper. The 2D barcode means 2-dimensional barcode that contains more information than conventional 1-dimensional barcodes. Conventional barcode gets wider as more data is encoded, but 2-dimenstioanl barcodes make use of the vertical dimension to pack in more data. 2D barcode is widely used to identify physical products and designed to endure various physical damage.

From several 2D barcodes, DataMatrix [9] is adopted in this paper. DataMatrix is an efficient 2D barcode symbol that uses a unique square module perimeter pattern that helps the barcode scanner to determine the cell locations. It can encode any kind of data including a letter, numbers, text and binary data. The DataMatrix symbol is square and can range from 0.001 inch per side up to 14 inches per side. It also supports advanced encoding and error checking with Reed Solomon error correction algorithms, named ECC200 [9]. This mechanism allows the recognition of barcodes that are up 60% damaged. From this reason, the watermark using DataMatrix can be survived other than ordinary cipher images in highly noisy environments.

## 3. Structure

### 3.1 Watermark Insertion

The Watermark Insertion System is a form of Content Distribution Network (CDN) [13] applications installed on Web server. Whenever consumers issue a download request, the Insertion System takes user-ID, user's IP, time stamp, and Content Provider's ID to create a Tag shown in Fig.1.

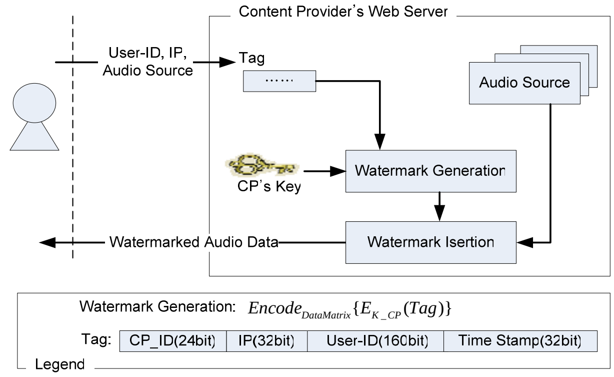


Fig. 1 Watermark Insertion System

Content Provider's ID is 24 bits value that is used to identify from other content providers adopting this system after decryption. Then, the Insertion System encrypts the Tag with Content Provider's 128 bits key using DES [14]. Encryption of these data prohibits hackers to counterfeit its original value. After encryption, it generates a 2D barcode watermark from the encrypted data. After making the 2D barcode watermark, the Insertion System inserts this watermark into requested audio source. Therefore downloaded audio source may have a little bit different byte streams whenever download is occurred.

### 3.2 Watermark Embedding

The proposed algorithm in this paper inserts watermarks in the wavelet domain. A 2D barcode image is used for watermark. In general, a logo, seal or signature is used for watermark to prove copyright and these are presented as a binary image.

Embedding steps are summarized as follows.

1) Let $M_1 \times M_2$ be the 2D barcode image's size. For the prevention of deformation or detection of watermark, a watermark is scrambled using pseudo-random sequence that has deterministic random characteristics and statistical measurements such as Eq. 1.

$$w = \{w(k), k = 1,2,\dots,N, \quad N = M_1 \times M_2\} \qquad (1)$$

Where $k$ is relocated by pseudo-random sequence and $w$ is 2D barcode image sequence for watermark and $N$ is the size of watermark sequence. Also $N$ is the size of a segment of audio signal in which the DWT is applied and one bit code is embedded in each segment [8][11][12].

In the proposed algorithm in this research, watermark embedding process is composed as following sequences; the segmentation, the wavelet transform of each segmentation, coefficient selection, watermark embedding and inverse wavelet transform (Fig. 3.).

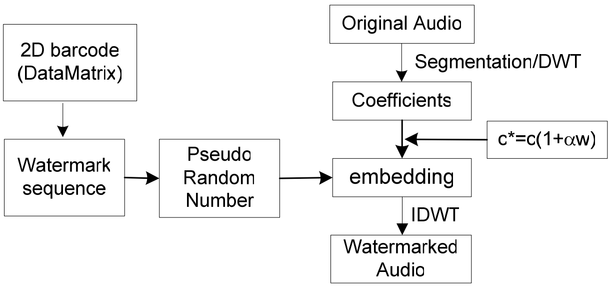


Fig. 2 Watermark embedding process using wavelet transform and 2D barcode

2) The audio signal is divided in segments of $N$ samples and each segmental audio signal, $x = \{x_1,\dots,x_N\}$ is

wavelet decomposed to the $L^{th}$ level. Suppose $c$ is the biggest coefficients' absolute value of wavelet coefficients in the detail parts of $L^{th}$ level. Watermark is embedded to the wavelet coefficient using Eq. 2.

$$c^* = c(1 + \alpha(k)w) \qquad (2)$$

$c^*$ is the watermarked wavelet coefficient and $\alpha(k)$ is an embedding weight of the $k^{th}$ segment and a constant which controls the amplitude of the watermark signal. Eq. 2 is used for embedding watermark adaptively based on the selected wavelet coefficient. That is, in case of large wavelet coefficients, a large $\alpha$ value is embedded and in case of small wavelet coefficients, a small $\alpha$ value is embedded. Watermark robustness generally increase with the watermark signal amplitude, $\alpha$ . Each audio segment embeds this value into itself as shown in Fig. 4.

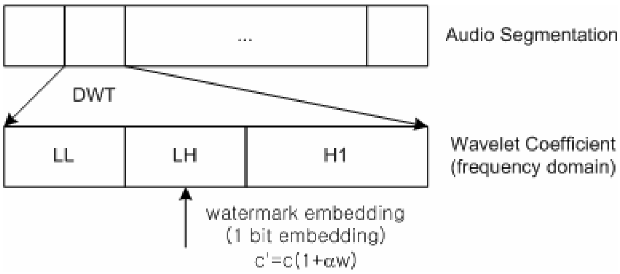


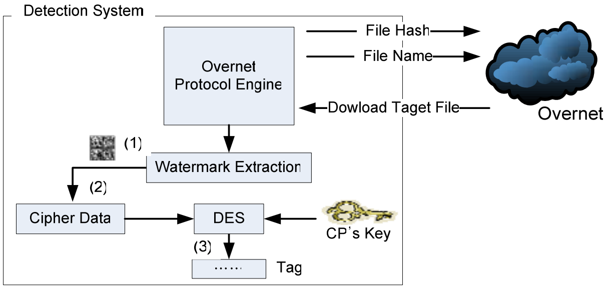
Fig. 3 Detailed embedding structure

3) According to the adjusted wavelet coefficients, recover the audio signal segments by IDWT. The recovered watermarked signal is $x^* = \{x_1^*, \ldots, x_N^*\}$ .

### 3.3 Watermark Detection

To detect unauthorized distribution of audio contents on P2P networks, a Watermark Detection System is designed. The Detection system embeds Overnet [15] protocol, so it able to join Overnet network like other normal clients such as eMule [16]. Since the Overnet P2P network supports fast download using distributed hash table and has tremendous digital contents, a lot of P2P users join the network. The Overnet splits file into several chunks and used these chunks as unit of transmission.

When content providers issue a searching request to the Detection System, it issues a query containing file's MD5 hash or file name to the Overnet. If the Detection System finds the target file, it downloads the file and extracts a 2D barcode image watermark from the file (Step 1. in Fig.4). The extracted 2D barcode image is decoded using Decode$_{\text{DataMatrix}}$() decoding function. The function translates 2D barcode into binary data (Step 2. in Fig.4). This binary data is decrypted with a Content Provider's Key (Step 3. in Fig.4) to get a Tag. After getting the Tag, the Detection System checks Content Provider's ID and distributor's information.



$$Tag = Decode_{DataMatrix}\{D_{K\_CP}(Cipher\_Data)\}$$

Fig. 4 Structure of detection

## 4. Evaluation

### 4.1 Test Environment

In this section, experimental results for various sounds and attacks are summarized. To evaluate the proposed algorithm, cipher image and cipher 2D barcode image are selected as watermark as shown in Fig. 5. Tag is encrypted and the result value is changed to hexadecimal string. This string is drawn in cipher image and encoded DataMatrix 2D barcode. The size of cipher image is 128 x 64 pixels and the size of cipher 2D barcode is Watermark image is 68 x 68 binary image. Daubechies-4 family wavelet filters are used for wavelet decomposition. After the audio signal is decomposed to 2 levels, wavelet coefficients in detail parts are selected for watermark embedding in each segment. Three audio sources are selected as Table 1. Two sources are classical music and one is pop music. Inaudibility and robustness of 2D barcode watermark is used for measurement of performance in this research. SNR is used for performance of the inaudibility after embedding watermark. Similarity using Eq. 2 is used for performance of the robustness.

Fig. 5 sample cipher image and cipher 2D barcode used for watermarking

### 4.2 Inaudibility

After embedding watermark to original audio, SNR are calculated for observing audio distortion as Table 1. From SNR in the Table 1, damages of audio signal are not recognized after applying the proposed algorithm for watermark.

Table 2: SNR of watermark embedded audio signal

| Audio | Classic: Beethoven – Sonata, No. 9 | Rock: White Lion – When The Children Cry | Jazz: B.B.King – Sweet Sixteen |
|---|---|---|---|
| Length | 3 min 59 sec | 4 min 00 sec | 4 min 00 |
| File size | 20.1 MB | 20.1 MB | 20.1 MB |
| SNR(dB) | 35.1 | 37.4 | 35.3 |

### 4.3 Robustness

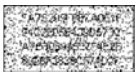
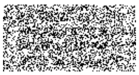
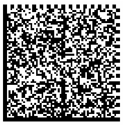
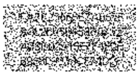
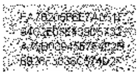
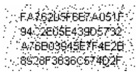
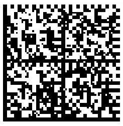
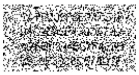
To test the robustness of the algorithm against various types of manipulations, the following types of signal processing were employed.

1) Down-sampling
The watermarked audio signals with a sampling rate 11.025 kHz were reduced to 11.05 kHz.

2) Lossy Compression
The robustness against the low-rate compression was tested by using MPEG 1 Layer III at 64kbps. Since the unexpected number of zeros is added at the front of audio signal during compression, a preliminary work to obtain the information about the start position of watermarking was done.

The experimental results are given in Table 2 which shows that watermark using the 2D barcode is not affected by down-sampling and lossy-compression. Good error-correcting with 2D barcode itself can enhance watermark detection.

Table 3: Results after attacks

| Audio Source | Attacks | Detected Cipher Image | Detected Cipher 2D Barcode | Decoding |
|---|---|---|---|---|
| Classic | MP3 |  | | Success |
| Rock | |  |  | Fail |
| Jazz | |  | | Success |
| Classic | Down Sampling |  | | Success |
| Rock | |  |  | Success |
| Jazz | |  | | Success |

## 5. Conclusion

In P2P networks, a lot of users illegally share tremendous digital audio contents. However, existing DRM systems can not provide effective solution about that. We proposed a watermarking platform for protecting unauthorized content distribution in P2P networks. The proposed platform dynamically generates 2D barcode watermark according to consumer's data and inserts the watermark into downloaded audio source in wavelet domain.

In the evaluation, ordinary cipher image and cipher 2D barcode image are used as watermark. These two groups of watermarked audio sources are attacked using MPEG-1 Layer III and re-sampling methods. These attacked audio sources are shared in the Overnet network for testing detection. From the experimental result, the proposed algorithm shows better inaudibility and robustness performance with comparing with the algorithms using cipher image as watermark.

Although the proposed watermarking platform is not able to prohibit illegal usage of digital audio content, it provides an effective method of easily tracing digital pirates on the P2P network. In the future, proper watermarking scheme adopting 2D barcode for image and video contents will be researched.

## References

[1] White Paper: Architecture of Windows Media Rights Manager," Microsoft, May. 2004.

[2] Koenen.R.H.., Lacy,J., Mackay.M., Mitchel.S, "The Long March to Interoperable Digital Rights Management," Proceedings of IEEE, vol.92, no.6, pp.883-897, Jun. 2004.

[3] "White Paper: Electronic Media Management System," IBM Web site, "http://www.microsoft.com/software/emms", 2004.

[4] Dubl.J, Kevorkian.S., "Understanding DRM System: An IDC White Paper," IDC, 2001.

[5] Nasir.M., Ping.W.W, "Protecting Digital Media Content," CACM, vol.41, no.7, pp.35-43, Jul.1998.

[6] Wolosewicz.J, "Apparatus and method for encoding and decoding information in audio signals," US patent 5.774.452,1998.

[7] Bender.W., Gruhd.D.,Lu.A., "Techniques for data hiding", IBM System Journal, vol.35. no3, pp.313-336, 1996.

[8] Gruhl.D., Lu.A., Bender.W., "Echo hiding," Info Hiding 96, pp.295-315, 1996.

[9] "Information technology – International symbology specification – Data Matrix," ISO/IEC 16022, Dec., 2004.

[10] Ghosemajumder. S., "Advanced peer-based technology business models," report, Sloan School of Management, MIT, 2001.

[11] Xueyao Li, Min Zhang, Rubo Zhang, "A New Adaptive Audio Watermarking Algorithm," Proceeding of the 5th World Congress on Intelligent Control and Automation, June 15-19, 2004, Hangzhou, P.R. China, pp. 4357-4361, June 2004.

[12] In-Kwon Yeo and Hyoung Joong Kim, "Modified Patchwork Algorithm: A Novel Audio Watermarking Scheme," IEEE Trans. on Speech and Audio Prcessing, vol. 11, no. 4, pp.381-386, July 2004.

[13] Peng, G. "CDN: Content Distribution Network," Technical Report TR-125, Experimental Computer Systems Lab, Dept. of Computer Science, State University of New York, Stony Brook, NY 2003.

[14] Raymond, G. K., "Data Encryption Standard (DES)," Federal Information Processing Standards Publication, 1995.

[15] Bhagwan, R. and Voelke, GM, "Overnet: Understanding Availability," Proc. of the 2nd International Workshop on P2P Systems, 2003.

[16] Kulbak, Y. and Bickson, D, "The eMule Protocol Specification," Lecture Notes of School of Computer Science and Engineering, The Hebrew University of Jerusalem, 2005.

**Eui-Hyun Jung** received the B.S., M.S. and Ph.D. degrees in Electronic Engineering from Hanyang University, Seoul, Korea, in 1992, 1994, and 1999, respectively. He joined Daewoo Communications, Seoul, Korea, in 1999. Presently, he is with in the Dept. of Digital Media, Anyang University as a full lecturer, Anyang City, Korea since 2003. He is presently interested in Wireless Sensor Networks, P2P and Semantic Web.

**Seong-Yun Cho** received the B.S. and M.S. degrees in Electrical Engineering from Hanyang University in 1987 and 1989, and Ph.D. degree in Computer Systems Engineering from University of Wales, Cardiff in 1999 respectively. During 1989-1994, he stayed in Korea Telecom Research Center (KTRC), to study digital communication system program, B-ISDN administration and Management module. He is now with Anyang University Digital media department as associate Professor.