

An Robust Watermarking Algorithm based on Coefficients Group Quantization

WenJi Quan¹, De Li^{1*} and JongWeon Kim²

¹ Department of Computer Science, Yanbian University, Yanji, China

² Department of Copyright Protection, Sangmyung University, Seoul, Korea

moongill2008@163.com, leader1223@ybu.edu.cn, jwkim@smu.ac.kr

*Corresponding author: De Li (leader1223@ybu.edu.cn)

Abstract

With spreading of digital contents, stealing other's properties by unpermitted people have become easier. In order to protect the legitimate rights of owners, the digital watermark technologies are becoming more popular. In this paper, we propose an audio watermarking algorithm based on DCT coefficients and audio feature quantization. The proposed algorithm protects watermark information using several factors, such as filtering, audio feature extraction formula, quantization value, etc. Furthermore, in order to evaluate the performance of our proposed algorithm, we experiment our algorithm under the attacks such as low pass filtering, noise addition, and compression. From the experiment result, we can see that the proposed algorithm has high robustness.

Keywords: Audio watermarking, Audio feature, DCT, Quantization, Robustness

1. Introduction

With the advent of the information age, there are a lot of information transmitted using digital forms such as text, images, audio and video. It is practically difficult to secure and protect the content author or owner's legitimate rights for digital audio from being stolen or copied because of its size and easy transmissible feature. This has given rise to an urgent need for protecting owner's copyright and information. Digital watermarking technology is being developed to meet this need. Digital watermarking technology is the process which embeds a signature of the copyright owner, into digital signals and verifies the proprietary right by extracting the embedded signature [1-2]. To extract the correct embedded signal and ensure the quality of original digital content, digital watermarking technology has to satisfy the some requirements, such as perceptual transparency, security, robustness, etc. [3-4]. Perceptual transparency is one of the most important parameters in watermarking technology. It means that the embedded watermark should not affect the original signal quality. Security is the second parameter for evaluating watermarking algorithm. If the watermark signal is easily attacked by the attacker, then the algorithm will be useless. Robustness is another parameter to evaluate watermarking algorithm behavior, which means we can detect the watermark after the watermarked signal is processed by common signal processing. However, these kinds of parameters interact with each other. So the proposed watermarking algorithm must consider all the important parameters.

In order to protect the copyright of digital signal, several watermark algorithms has been proposed. However, most of watermarking signatures were embedded in images, and a few algorithms focused on audio and video [5-16]. The previous proposed audio watermarking

algorithms can be grouped into three categories: Patchwork in the frequency domain, echo hiding in the time domain, and spread-spectrum. The previous audio watermarking algorithms have mostly concentrated on improving the robustness under the variety of audio attacks. But the robustness performance under compression is still not good and easy to attacks.

In this paper, we use the DCT coefficient and feature group quantization to implement our algorithm. First of all, in proposed algorithm, we extract the values of low-frequency and middle-frequency from the DCT performed audio signal. Next, we calculate audio feature with the extracted coefficient. Finally, we get the embedding strength of each audio segment, and embed a watermark signature with the proposed equation. In order to evaluate the proposed algorithm, we implement proposed algorithm using MATLAB. From the experiment result, we can see that our algorithm has high robustness under the normal audio attacks such as low pass filtering, noise addition, and compression. The proposed algorithm has high robustness particularly for the compression attacks.

This paper is organized as follows. In Section 2 we discuss the previous audio watermarking technologies and in Section 3, we give the basic theory of the embedding strength and its calculation, and Section 4 describes the algorithm for embedding and extracting the watermark signature. Section 5 describes and analyzes the simulation result. Finally, we present our brief conclusions in Section 6.

2. Related Work

In order to protect the watermark information in the audio signals, a few audio watermarking algorithms have been proposed. [5] proposed an audio watermarking algorithm that exploits temporal and frequency masking by adding a perceptually shaped spread-spectrum sequence. However, in this scheme, the original audio signal is needed in the watermark detection process. [6] introduced a watermark algorithm based on spread spectrum coding, which uses a linear predictive coding technique and Fast Fourier Transform (FFT) to determine the spectral shape. However, in the watermark detection process, the proposed scheme needs to whiten before correlation. [7] represented a new concept of audio watermark. The basic idea is that it partly decodes the input bit stream, and adds a perceptually hidden watermark in the frequency domain. Finally, it quantizes and codes the signal again. Different from previous watermarking methods based on time domain, [8] proposed a robust watermark algorithm that embeds a watermark into an audio signal which is modified in time domain. The characteristics of this modification were determined both by the original and the copyright owner key.

In our proposed watermarking algorithm, we detect the watermark information using the feature quantization table. The feature quantization table is a secret key that can improve the security of the proposed algorithm. Furthermore, in order to improve the robustness of the watermark, we decide the frequency domain to embed the watermark. The simulation result shows that our algorithm has high robustness and several components to protect the watermark information.

3. Fundamental Theory of Embedding Strength

In our proposed watermarking scheme, the watermark signature can be embedded into the original audio by following steps. Firstly, the audio signal is segmented according to the length of the watermark information. Secondly, DCT is performed on those selected segments, and the procedure extracts the low frequency and middle frequency, which is used for

calculating the embedding strength of each segment. Finally, the watermark embedding scheme is implemented using the calculated embedding strength value.

3.1. Basic Concept of the Embedding Strength

In order to improve robustness of the watermark, we use the embedding strength. The embedding strength is calculated by the audio features and quantization tables. Figure 1 represents the concept of the embedding strength calculation.

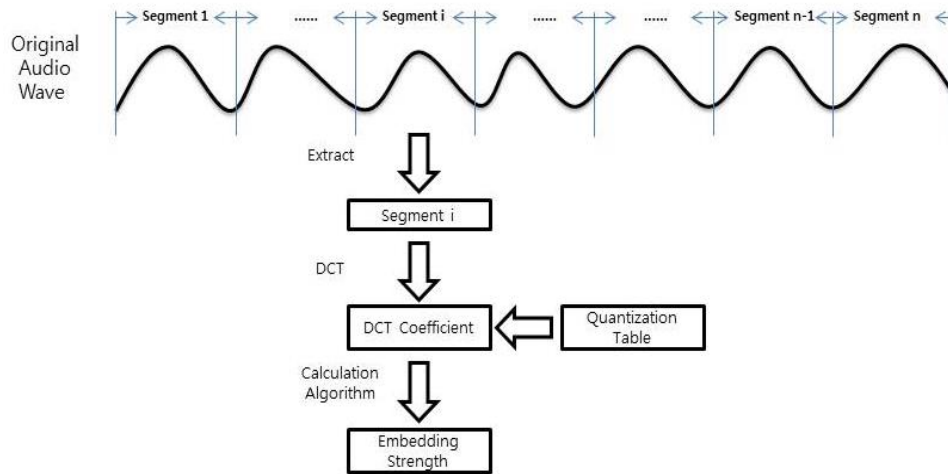


Figure 1. The Concept of the Embedding Strength Calculation

Figure 1 shows that after segmenting the original audio signal, the procedure extracts a small amount of values from each segment and performs DCT on each segment. After applying DCT, using the proposed embedding strength calculation algorithm and quantization table, we can finally obtain the embedding strength of each segment. The following section will describe the calculation of the embedding strength in more detail.

3.2. Embedding Strength Calculation

In order to calculate the embedding strength of the each segmentation, we split the original audio signal according to the length of the watermark information. Then, we extract low-frequency and middle-frequency coefficients after the DCT is performed. Next, we calculate the embedding strength of each segment using the coefficient values. The following steps represent the embedding strength calculation.

- [1] In order to embed one bit into each segment, we split the original watermark signal into blocks, according to the length of the watermark information.
- [2] After splitting the signal, we transform each block to two dimensions. And then, DCT is performed on two dimensions of each block.
- [3] Choose low frequency and middle frequency coefficients; compose these coefficients to a sequence.
- [4] Divide the sequence equally into groups “A” and “B”. Using equation (1) and equation (2), calculate “ S_A ” and “ S_B ”, which represent the characteristic values of the group A and group B.

$$S_A = \sqrt{\frac{1}{N} \sum_{t=i-1}^{t=i-\frac{1}{2}} S(t)^2} \quad (1)$$

$$S_B = \sqrt{\frac{1}{N} \sum_{t=i-\frac{1}{2}}^{t=i} S(t)^2} \quad (2)$$

In equation 1 and equation 2, $S(t)$ represents the combined value and N represents the length of $S(t)$.

- [5] Calculate the audio feature F with S_A and S_B using equation 3. The audio feature F represents the characteristic value of the audio segment.

$$F = \frac{S_A - S_B}{S_A + S_B} \quad (3)$$

- [6] Quantitate the feature value F with the quantification tables. In our algorithm, we set the quantization table as Q_0 , and Q_1 . If the watermark signal is 0, then we quantify the feature with Q_0 , else with Q_1 .

$$Q_0 = \{-0.7, -0.3, 0.1, 0.5, 0.9\}$$

$$Q_1 = \{-0.9, -0.5, -0.1, 0.3, 0.7\}$$

- [7] Calculate the embedding strength with equation 4, where Q represents the quantized value and F represents the audio feature.

$$g = \frac{1}{2} \frac{Q - F}{1 - QF} \quad (4)$$

4. Embedding and Detection Watermark Scheme

In our proposed watermark embedding algorithm, in order to improve the performance of the robustness, we embed the watermark signature into the low frequency and middle frequency domain of DCT coefficients. Furthermore, we use the quantization table, which can improve the security of the proposed algorithm. In addition, in watermark detection process, we can detect the watermark information without original audio signal so that the proposed algorithm has high availability.

4.1. Watermark Embedding Scheme

The proposed watermark algorithm is based on audio feature quantization. At the first time, we calculate the feature and embedding strength of audio with the proposed equations, and use the following embedding algorithm to implement the embedding scheme.

The main steps of the embedding procedure can be described as the following steps:

1. Split the original audio signal according to the length of watermark signature. After splitting, extract 640 coefficients from each segment. The reason why we extract 640 coefficients is that we generate a 64 bits random signal as our watermark information and embed one bit of watermark into a segment.

2. Reshape each 640 coefficient to $8 \times 8 \times 10$ blocks and 2D-DCT is performed on each 8×8 block. Extract 10 coefficients of low frequency and middle frequency coefficients from 2D-DCT performed blocks. The following figure 2 represents the detail process of the reshape.
3. Compose 100 coefficients and divide it to two parts. Using the equation 1 and 2 calculate S_A and S_B .
4. Calculate each segment feature with equation 3. If the watermark bit is 0 then quantify the feature with the nearest value in Q_0 , else quantify with the nearest value in Q_1 . Equation 5 represents the audio feature quantization.

$$F \approx \begin{cases} Q_0 W_m = 0 \\ Q_1 W_m = 1 \end{cases} \quad (5)$$

where W_m represents the watermark information, and Q_0 and Q_1 represents the quantization tables.

5. Calculate the embedding strength with the feature F and quantified value Q , using equation 4.
6. Embed the watermark using the following equation.

$$\begin{cases} A: s(t)' = s(t) + gs(t) \\ B: s(t)' = s(t) - gs(t) \end{cases} \quad (6)$$

Where $s(t)'$ represents the watermarked audio signal, g represents the embedding strength and $s(t)$ represents the original signal.

The watermark embedding procedure is shown in Figure 2.

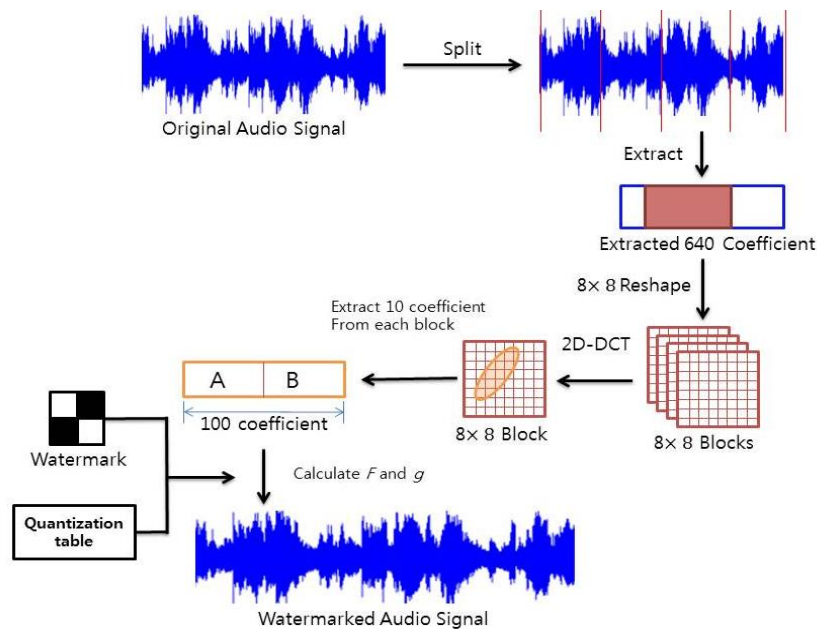


Figure 2. Watermark Embedding Scheme

4.2. Watermark Extracting Scheme

In order to extract the watermark information, we need the watermarked audio as well as the quantization table and watermark size information. The quantization table, which is used as a secret key, can improve the security of the algorithm. The watermark extracting process can be described as the following steps.

1. The watermarked audio is segmented according to the length of the watermark.
2. Extract the audio 640 coefficient from each segment, and divide it to 8×8×10 blocks.
3. 2D-DCT is performed in each 8×8 block, extract 10 coefficients of the low and middle frequency from each 8×8 block.
4. Combine the extracted coefficients and calculate the feature with the equation 3.
5. Compare the calculated feature with the member of table Q0 and Q1. If all the features are close to a member of group Q0, then we extract “0”, else extract “1”. Equation 7 represents the watermark extraction.

$$w_m = \begin{cases} 0 & F \approx Q_0 \\ 1 & F \approx Q_1 \end{cases} \quad (7)$$

Where W_m represent the watermark and F represent the calculated audio feature.

Figure 3 represent the watermark extracting process.

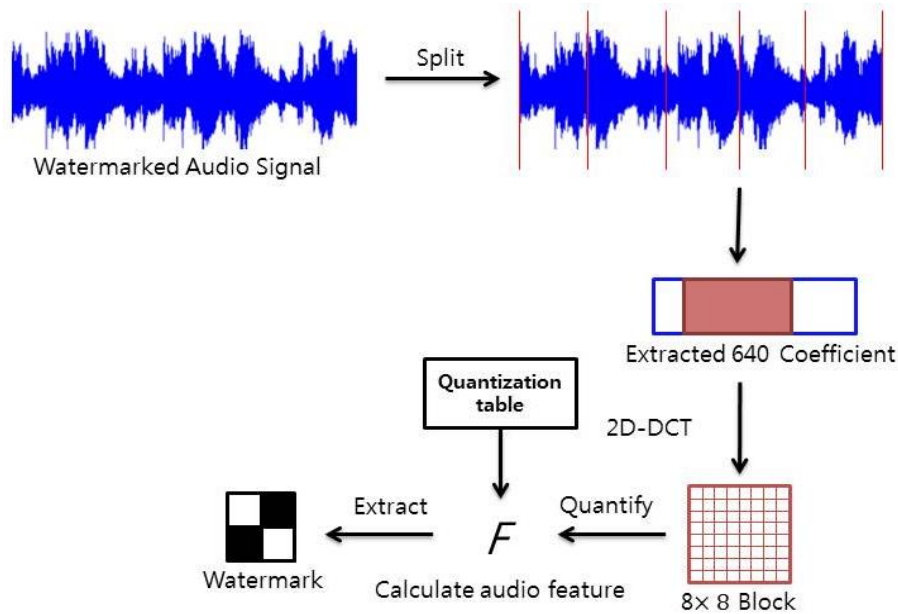


Figure 3. Watermark Extracting Scheme

From Figure 3 we can know that the watermark extracting algorithm is the reverse process of the watermark embedding algorithm. In order to extract the watermark information, we need to save some values, such as the size of the watermark, quantization table, embedding position, *etc.* These kinds of values can become a secret key that can improve the security of the proposed algorithm.

From the watermark embedding and extracting algorithms, we can know that the proposed algorithm not only has variety of factors, which can protect the watermark from being stolen, it can also protect the watermark with the several steps of embedding process. In the next section, we implement the proposed algorithm and test the performance of our algorithm under some attacks, such as low pass filtering, noise addition, and compression.

5. Simulation Result

In order to illustrate its inaudible and robust nature, we have implemented the proposed watermarking scheme on digital mono audio signals of 10s in length using MATLAB. We used the randomly generated 8×8 bit binary image as our watermark. In order to evaluate the performance of the proposed watermarking algorithm, we used the StiramrkForaudio v2.0, which is a software widely used to test the robustness of audio watermark. The proposed algorithm has been implemented in the simulation environment as shown in Table 1.

Table 1. Watermark Detection Results for Common Signal Processing

Parameters	Value
Software	Matlab 2011a
Audio Length	10s
Watermark	64bit
Test tool	StiramrkForaudio 2.0

Figure 4 shows the watermark signature that we used in this paper.

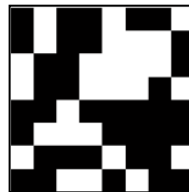


Figure 4. Watermark Signature

Besides, we considered the case that the audio signal may be suffered several kinds of attacks while it is spreading through the Internet, and tested the BER values after the attacks, such as RC low pass filtering, noise addition and compression. The BER can be defined as equation 6.

$$BER = \frac{B}{M \times N} \times 100\% \quad (6)$$

Where B represents the number of erroneously detected bits and M×N is the size of the watermark.

Table 2 shows the BER values of the proposed algorithm under the mentioned attacks.

Table 2. Watermark Detection Results for Common Signal Processing

Signal Processing	BER
No processing	0%
RC low pass	4%
Noise addition	1%
Compression	3%

From the Table 2, we can see that with the attack of no processing, we could correctly extract the watermark signal. Besides, with the RC low pass filtering and noise addition attacks, the proposed algorithm could extract the watermark signals with below 5% BER values. It is means that the proposed watermark algorithm has high efficiency. Finally, with the compression attack, the BER is 3%, which means that our algorithm has high usability under compression attack.

In addition, we implemented our watermarking algorithm with several kinds of audio styles. Table 3 and Table 4 represent the SNR and BER values of the several styles of audio.

Table 3. Data for the Different Music Styles Tested

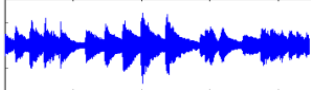
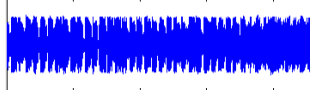
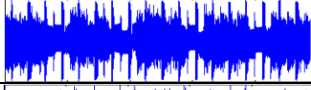
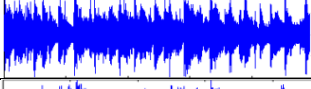
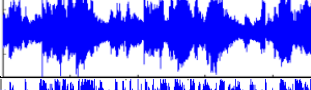
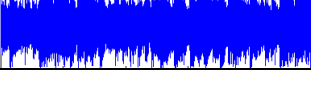
Audio content	SNR (dB)	Sample audio signal
Classical	34.31	
Dance	40.53	
Hip hop	44.29	
Jazz	34.75	
R & B	38.50	
Rock	40.69	

Table 3 shows the SNR values of the different audio styles. From the table, we can see that the proposed watermarking algorithm has high SNR after the watermark signature is embedded. After test SNR, we test BER from the attacked audio signals. The following table shows the results of BER of the different audio styles.

Table 4. Watermark Detection Results for Different Music Styles

Audio style	BER			
	No processing	Low pass	Noise addition	Compression
Classical	0%	4%	1%	1%
Dance	0%	3%	1%	3%
Hip hop	0%	4%	0%	6%
Jazz	0%	3%	1%	3%
R & B	0%	1%	0%	4%
Rock	0%	1%	1%	7%

From Table 4, we can see that with no attacks we could correctly extract the watermark information from all the audio styles. And, with the low pass filtering attack, even some of the watermark information was missed, but the BER values were smaller than 5%, which means that our algorithm has high robustness under low pass filtering attacks. Also, in the case of noise addition attack, the BER values were high enough to cover the missing value. In addition, in the case of the compression attack, although the BER values are a little higher than the other attacks, but the BER values still could be covered by the error control mechanisms.

From the above experiments, we can prove that the proposed watermarking algorithm is very useful to protect the copyright of content owners. Furthermore, in the embedding algorithm, we use variety of parameters to improve the security of the algorithm. And we embed 64bit of watermark signal into 10s mono audio signals, which means that if the audio signal is long enough, we can embed a large amount of copyright information to one audio. So our algorithm can satisfy the requirements of the watermark technology.

6. Conclusion

In this paper, we have proposed a robust watermark algorithm based on audio feature quantization. The robustness of the algorithm is a result of three main steps: audio feature calculation, embedding strength calculation, and watermark embedding scheme. Audio features are quantized using the quantization tables, and calculate the embedding strength with audio feature and quantitated values. From our experimental findings, the proposed watermark algorithm achieved robustness against common audio signal processing techniques, especially for compression attack. From the simulation results, we can see that the SNR values of the watermarked audio were higher than 33dB and BER values were lower than 7%. In addition, the watermarks could be extracted without original audio signal, thus, the proposed watermark has high usability. Besides, in order to improve the security of the proposed algorithm, we used several kinds of the security parameters, such as watermark size, quantization table, embedding area, *etc.* These kinds of values can be used as a secret key stored in the system. If attackers are unable to get the information about these values, it will be hard for them to get the watermark information.

Future research will focus on improving the performance of the algorithm to enhance the robustness and reduce the impact on original audio.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 61262090).

References

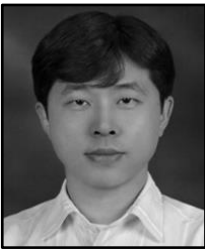
- [1] I. J. Cox and M. L. Miller, "The first 50 years of electronic watermarking", *J. Appl. Signal Process.*, vol. 56, no. 2, (2002), pp. 225-230.
- [2] The Wiki website, (2012), http://en.wikipedia.org/wiki/Digital_watermarking.
- [3] J. Kim, *et al.*, "Watermarking two dimensional data object identifier for authenticated distribution of digital multimedia contents", *Signal Processing: Image Communication*, vol. 25, (2002), pp. 559-576.
- [4] J. Seok, J. Hong and J. Kim, "A Novel Audio Watermarking Algorithm for Copyright Protection of Digital Audio", *ETRI Journal*, vol. 24, (2002), pp. 181-189.
- [5] M. Swanson, B. Zhu, A. Tewfik and L. Boney, "Robust Audio Watermarking Using Perceptual Masking", *Signal Processing*, vol. 66, no. 3, (1998), pp. 337-355.
- [6] C. Lee, K. Moallemi and R. Warren, "Method and Apparatus for Transporting Auxiliary Data in Audio Signals", U.S. Patent 5,822,360, (1998) October.
- [7] C. Neubauer and J. Herre, "Digital watermarking and its Influence on Audio Quality", 105th AES Convention, Audio Engineering Society preprint 4823, San Francisco, (1998) September.
- [8] P. Bassia, I. Pitas and N. Nikolaidis, "Robust Audio Watermarking in the Time Domain", *IEEE Trans. On Multimedia*, vol. 3, (1999).
- [9] S. W. Shin, J. W. Kim and J. U. Choi. "Development of Audio Watermarking Algorithm using Audio Feature Quantization", *Telecommunication Review*, no. 5, (2002) October, pp. 653-662.
- [10] X. -Y. Wang, P. -P. Niu and H. -Y. Yang, "A robust digital audio watermarking based on statistics characteristics", *Pattern Recognition*, vol. 42, no. 11, (2009).
- [11] J. S. Seo, M. Jin, D. Jang, S. Lee and C. D. Yoo, "Audio Fingerprinting Based on Normalized Spectral Subband Moments", *IEEE Signal Processing Letters*, vol. 3, (2006), pp. 209-212.
- [12] C. J. C. Burges, J. C. Platt and S. Jana, "Distortion Discriminant Analysis for Audio Fingerprinting", *IEEE Transactions on Speech and Audio Processing* (2001) December.
- [13] H. Yang, X. Jiang and A. C. Kot, "Image watermarking using dual-tree complex wavelet by coefficients swapping and group of coefficients quantization", *IEEE 2010 Conference on Multimedia and Expo*, (2010), pp. 1673-1678.
- [14] D. Li, Y. Ji and J. Kim, "Audio Watermarking by Coefficient Quantization in the DWT-DCT dual domain", *Advanced Science Letters*, (2012).
- [15] I. K. Yeo and H. J. Kim, "Modified patchwork algorithm: A novel audio watermarking scheme", *IEEE Transactions on Speech and Audio Processing*, vol. 11, no. 4, (2003), pp. 381-386.
- [16] D. Gruhl, A. Lu and W. Bender, "Echo Hiding", *Proc. of 1st Information Hiding Workshop, LNCS vol. 1174*, Berlin, Germany: Springer-Verlag, (2001), pp. 295-315.
- [17] L. Cui, S. Wang and T. Sun, "The application of binary image in digital audio watermarking", *Neural Networks and Signal Processing*, vol. 2, (2003), pp. 1497-1500.

Authors



Wenji Quan

He is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas of text document copyright protection, text image copyright protection, information security and digital watermarking.



De Li

He received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.



JongWeon Kim

He received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a professor of Dept. of Copyright Protection at Sangmyung University in Korea. He has a lot of practical experiences in the digital signal processing and copyright protection technology in the institutional, the industrial, and academic environments. His research interests are in the areas of copyright protection technology, digital rights management, digital watermarking, and digital forensic marking.

