Hardware Based Real Time Audio Watermarking Using Embedded Module

Jung-Hee Seo, Hung-Bog Park

1, First Author Dept. of Computer Engineering, Tongmyong University, jhseo@tu.ac.kr
2, Corresponding Author Dept. of Computer Engineering, Pukyong National University, git@pknu.ac.kr

Abstract

To achieve audio signal robustness, this paper proposed a blind watermarking algorithm that embeds watermark in coefficient bits of the low frequency band and extracts it without original audio signal. It spreads the frequency band for hardware based watermarking to protect audio contents rights, generates watermark sequence on the watermark key using block code, and embeds and extracts watermark in the audio signal. It is implemented on the Blackfin processor using embedded module based LabView. Implementation in the high level language such as the graphical language over the low level architecture demonstrates the balanced method in high level and low level programming. By this test environment, it is possible to easily modularize and expand. In addition, it is possible to prototype promptly, and the Blackfin processor used in this experiment is suitable for real time audio signal processing. Therefore, equipments combined with digital watermarking facilitate insertion and extraction of watermark for variety contents and guarantee an intellectual ownership right of digital contents.

Keywords: Watermarking based on Hardware, Blind Audio Watermarking, Wavelet, Spread Spectrum

1. Introduction

As the Internet has rapidly grown, it is to download digital contents not only from computers but also various mobile devices, and it is possible to copy or tamper them with relatively simple tools. As such, losses in the contents industry such as video and audio contents have increased every year. Consequently, concern on intellectual property protection for digital contents has increased, and lots of studies have been introduced related to digital watermarking as an intellectual ownership protection.

The DRM(Digital Rights Management) system is essential to establish rights, to trace users, to ensure access, to protect illegal copy and to promote contents authentication[1].

Most of existing studies developed software based watermarking algorithms, and studies on such form of watermarking have entered the mature phase. However, recent studies are introducing hardware based watermarking algorithms, yet in the enfant phase compared to software based watermarking methodology. Integration of existing electronic devices and watermarking chips supports these to achieve real time performance[2].

General objective of hardware based watermarking is to achieve low power consumption, real time performance, stability and easy integration with existing user electronic devices. Moreover, hardware implementation can enhance restriction in capacity and search time better than software implementation[3].

Recent studies are proposing hardware based watermarking algorithms. However, hardware integration related to audio watermarking is far behind. Yet, technology is developed in the level that some phone services recognize user voice.

One of typical examples is financial transaction application using mobile phone. Suppose that a financial service provider transmits important goods information to a user’s mobile phone and performs safe transaction. The banking sector requires the mobile phone banking system for more and more new services noticeably. Main purpose in such kind of applications is speech authentication of speakers. However, identification by speech processing technology is not enough to authenticate speakers because their voices can be mimicked and cheat the system. Therefore, the digital watermarking method can be used to solve such problem. The digital watermarking method generates user’s watermark from the user or by modifying user’s specific data. Watermark embedding and
extraction in the mobile phone banking or financial service applications is conducted in real time. Thus, the mobile devices become targets for such algorithm implementation. However, hardware complexity in the embedding and extraction algorithms becomes a big issue[4].

On the other hand, important studies have performed DRM technology development mainly in the off-line for past couple of years. Before providing watermark images or videos to users, watermarks are inserted into multimedia data in advance followed by the existing plan. Such scenario fits in the off-line applications such as digital cinemas and digital libraries for example. However, the existing algorithmic approach and system is not appropriate for real time and computing intensive applications[1].

Hardware based watermark algorithm uses the blind watermarking method that does not rely on the original signal on watermark extraction to reduce system memory requirements.

In this paper, to achieve audio signal robustness, proposed is a blind watermarking algorithm that embeds watermark in coefficient bits of the low frequency band and extracts it without original audio signal. It spreads the frequency band for hardware based watermarking to protect audio contents rights, generates watermark sequence on the watermark key using block code, and embeds and extracts watermark in the audio signal. It is implemented on the Blackfin processor using embedded module based LabView.

Moreover, implementation in this paper uses high level graphical language such as LabView to design the watermark algorithm to be embedded in the hardware. Yet, it implements the watermark algorithm on the low level processor such as ADSP-BF537 Blackfin processor. It presents a balanced method in programming between proposed high level watermark algorithm and low level hardware implementation technology.

This paper structure is as follows. Section 2 reviews related studies on existing hardware based watermarking. Described are in the order of the audio watermarking algorithm based on the embedded module in section 3, implementation result and analysis in section 4, conclusion in section 5 and references at the end.

2. Hardware Based Watermarking

In the paper [5], the hardware support solution proposed for multimedia objects was studies. It was studied that hardware should be integrated with application problem in low power, real time performance, high reliability and low cost. It was also studied that either integrating the watermarking chip in the existing digital still image camera or integrating a JPEG codec in the hardware module was essential for integration with existing user electronic devices. The JPEG codec can be part of scanner, digital camera or other multimedia devices to watermark digitized images while capturing.

Existing hardware based watermarking systems[2, 6-9] are implemented on hardware such as DSP (Digital Signal Processor), IC (Integrated Circuit), FPGA (Field Programmable Gate Array), or ASIC (Application Specific Integrated Circuit).

FPGA technology was chosen by following strengths in implementation. (1) FPGA provides high density for arithmetic logic within relatively short time of design cycle. (2) In FPGA, it is possible to control operations at bit level to build specialized data paths[6].

The paper [7] discusses implementation of the robust non-visual binary image watermarking algorithm over FPGA and ASIC using connectivity preserving criteria. This algorithm is processed in the spatial area and prototyped on (i) XILINX FPGA and (ii) 130nm ASIC.

This algorithm is tested by Virtex-E (xcv50e-8-cs144) FPGA and implemented on ASIC. Software implementation of the watermarking algorithm is less useful if the image size and bit depth increases high. Therefore, hardware description languages (HDL) are used in implementation of media applications. The design is programmed with VHDL and can achieve needed performance. It can be downloaded on FPGA.

The paper [8] proposes new encryption system and it is possible to design and verify the VLSI structure. The new system performs both random positional permutations and random value conversion. The chaos system processes input data by swap and XOR/XNOR functions under control of the binary sequence. The highly modularized regular VLSI structure in low hardware cost and fast computing speed is implemented in the Altera FPGA in the Avanti cell library design to maintain real time requirements. Consequently, the newly proposed encryption system is very suitable for most of real time video and audio application programs.
3. Embedded Module Based Audio Watermarking Algorithm

This paper proposes the blind watermarking algorithm that extracts the watermark from the watermark sequence inserted in the audio signal without the original audio signal. In addition, to achieve audio signal robustness, the watermark is embedded in coefficient bits of the low frequency band and the watermark key is encoded by the block code based hamming code simultaneously. Accordingly, the watermark sequence is generated by frequency band dispersion and using the block code over the watermark key and then the watermark is embedded and extracted on/from the audio signal. The embedded module based LabView is used to implement it on the Blackfin processor.

3.1. Watermark Embedding

Figure 1 illustrates the watermark embedding algorithm for audio signal to be implemented on the Blackfin processor.

First, the ‘Initialize Audio Device’ step is processed. Here, it initializes the audio device drivers of BF537 EZ-Kit. That is, it initializes AD1854 and AD1871 device drivers of BF537 EZ-KIT. The number of data samples collected from the device before the device triggers interrupt is entered to the sample number to identify the device buffer. Then data is copied to the array from the device buffer (1871 Buffer).

In the ‘Digital Filter Design’ step, post audio signal processing is conducted.

In the ‘Watermark Key’ and ‘Encoding’ step, the watermark key is encoded based on the block code and the watermark sequence is generated.

In the ‘Wavelet Transform’ step, the wavelet transform based on the Daubechies4 equation is calculated over the audio signal (X). The Daubechies4 equation is defined as Equation (1) using the transformation matrix.

Equation (1) is the Daubechies4 equation for wavelet transformation and void inputs indicate zeros. Numbers $c_0$, $c_1$, $c_2$ and $c_3$ should satisfy the exact orthogonal property (Equation(2)).
\[
\begin{bmatrix}
   c_0 & c_1 & c_2 & c_3 \\
   c_3 - c_2 & c_1 - c_0 & c_0 & c_1 & c_2 & c_3 \\
   ... & \cdot & \cdots & \cdot & \cdots & \cdot & \cdots & \cdot & \cdots & \cdot & \cdots & \cdot \\
   c_3 - c_2 & c_1 - c_0 \\
   c_2 & c_1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
   c_2 - c_0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
   \end{bmatrix}
\]

(1)

c_0^2 + c_1^2 + c_2^2 + c_3^2 = 1 \\
c_2c_0 + c_0c_1 = 0 \\
c_3 - c_2 + c_1 - c_0 = 0 \\
0c_3 - 1c_2 + 2c_1 - 3c_0 = 0 

(2)

Along with Equation (3), it should satisfy \(c_0, c_1, c_2\) and \(c_3\) as the unique solution.

\[
\begin{align*}
c_0 &= \frac{1 + \sqrt{3}}{4\sqrt{2}} \\
c_1 &= \frac{3 + \sqrt{3}}{4\sqrt{2}} \\
c_2 &= \frac{3 - \sqrt{3}}{4\sqrt{2}} \\
c_3 &= \frac{1 - \sqrt{3}}{4\sqrt{2}}
\end{align*}
\]

(3)

Therefore, the Daubechies4 wavelet transformation over the array \(X\) is defined as follows.

\[
\text{Wavelet Daubechies4 } \{X\} = C \times X
\]

(4)

In the ‘Watermarking Embedded Algorithm’ step, the watermark sequence generated in the ‘Encoding’ step is embedded on the wavelet transformed coefficient bits.

In the ‘Inverse Wavelet Transform’ step, the wavelet inverse transformation is conducted to generate the watermark embedded audio signal. This signal data is copied to the device buffer (1854 Buffer) from the array. Then, the AD1871 driver resets the sub-buffer data ready flag. This step is used to return the sub-buffer index after waiting BF AD1871.

3.2. Hardware Implementation

In this paper, the test environment is implemented with the Blackfin processor on the ADSP-BF537 EZ-KIT Lite and development programs of graphical based LabView and VisualDSP++. Accordingly, the watermark algorithm is designed in the high level graphical language at the desktop computer, and re-code is generated and compiled in C language. It is embedded on the hardware to implement the application. The watermark extraction is simulated at the desktop computer.

Figure 2 illustrates the entire system architecture for the hardware to implement the watermark algorithm in this study.

The digital filter design and the watermark algorithm is designed to LabView based graphical language with using MSA(Micro Signal Architecture)-based embedded processor(Blackfin Processor), and designed algorithm is implemented in hardware after re-coded by using VisualDSP++.

The ADSP-BF537 EZ-KIT Lite is composed of an ADSP-BF537 Blackfin processor at maximum 600MHz clock speed, 64 Mbytes (32M × 16) SDRAM and 4 MB (2 M × 16 pixels) flash memory.
Table 1 shows the hardware implementation status of watermarks proposed in existing studies and this paper.

3.3. Watermark Extraction

In this paper, the audio signal was transformed into the wavelet based frequency band signal, and the watermark sequence is embedded on its coefficient bits. By dispersing the frequency band and inserting data in it, it enhances watermark robustness and imperceptibility and it enables blind watermarking extractable of the watermark key without the original signal.

In the experiment of this study, we can extract watermark sequences from coefficient bits in the certain frequency band after transformed in the wavelet based frequency band for the watermarked audio signal in common signal processing attacks. The extracted watermark sequences can be verified watermark keys after performing decoding based on the block code.

![Prototype System](image)

**Figure 2. Prototype System**

<table>
<thead>
<tr>
<th>contents</th>
<th>HW</th>
<th>Data Type</th>
<th>Watermark Type</th>
<th>Processing Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>paper [2]</td>
<td>FPGA</td>
<td>audio</td>
<td>invisible-robust</td>
<td>chip/Spread spectrum</td>
</tr>
<tr>
<td>paper [6]</td>
<td>FPGA</td>
<td>image/video</td>
<td>invisible</td>
<td>Wavelet</td>
</tr>
<tr>
<td>paper [7]</td>
<td>FPGA/ASCI</td>
<td>image</td>
<td>invisible-robust</td>
<td>Spatial</td>
</tr>
<tr>
<td>paper [8]</td>
<td>FPGA</td>
<td>video/audio</td>
<td>invisible</td>
<td>Spatial</td>
</tr>
<tr>
<td>Proposed method</td>
<td>embedded processor</td>
<td>speech</td>
<td>invisible-robust</td>
<td>Wavelet</td>
</tr>
</tbody>
</table>

4. Analysis of the Implementation

In general, the audio watermarking robustness is assessed on the original signal, the watermark embedded signal and the attacked audio signal by BER(Bit Error Rate) as shown in Equation (5). Its imperceptibility is assessed by SNR(Signal Noise Ratio) as shown in Equation (6).
Table 2 indicates imperceptibility analysis between SNR(dB) against general signal attacks by the methods in the existing papers [3] and [22], and that of this paper. [21] and [22] in Tables 2 and 3 are papers referenced in the paper [3] to compare and analyze performance.

Table 2. A Comparative Analysis of SNR(dB) for common signal processing attacks

<table>
<thead>
<tr>
<th>Attacks</th>
<th>SNR(dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Attack Watermarked</td>
<td>6.99</td>
</tr>
<tr>
<td>Re-quantization</td>
<td>3.62</td>
</tr>
<tr>
<td>Noise</td>
<td>3.62</td>
</tr>
<tr>
<td>Amplitude</td>
<td>6.99</td>
</tr>
<tr>
<td>MP3(128kbps)</td>
<td>4.78</td>
</tr>
<tr>
<td>Lowpass Filtering(12kHz)</td>
<td>2.76</td>
</tr>
</tbody>
</table>

In Table 2, SNR(dB) of 'No Attack Watermarked' represents an imperceptibility of watermarked signal which is embedded a watermark key on the original signal without signal processing attacks. The higher the SNR(dB) value is, the more imperceptibility and the more difficult it can be recognized from the original signal. However, a balance between imperceptibility and robustness has been a main issue since robustness, watermark extraction rate, decreases as imperceptibility increases. ‘Re-quantization’, ‘Noise’, ‘Amplitude’, ‘MP3(128kbps)’, and SNR(dB) of ‘Lowpass Filtering(12kHz)’ in Table 2 represent an imperceptibility of watermarked signal('No Attack Watermarked') against common signal attacks.
Since imperceptibility (SNR) of watermarked signals of the existing papers ([3], [21] and [22]) is assessed by 30dB in Table 3, the method prosed in this paper (Proposed method-1) was assessed robustness by 30dB (refer to Table 2) for performance analysis, as well. In addition, to analyze watermark extractability as increasing imperceptibility, Proposed method-2 in this paper assessed imperceptibility (SNR) of the watermarked signal at 47dB.

DR(%) in Table 3 shows that Proposed method-1 in this paper has higher watermark extractability than performance in the papers [21] and [22]. In the comparison with the paper [3], it showed almost similar extractability under No Attack Watermarked and Noise attacks. In addition, the audio watermarking robustness is generally assessed by BER(%), which was added in Table 3.

DR(%) of Proposed method-2 in this paper was assessed robustness against general attacks at 47.38dB SNR. It was observed that watermark robustness was decreased as imperceptibility increased, and BER(%) increased on the contrary.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No Attack Watermarked</td>
<td>83.2</td>
<td>82.1</td>
<td>100</td>
<td>99.66</td>
<td>98.89</td>
<td>0.34</td>
<td>1.11</td>
</tr>
<tr>
<td>Re-quantization</td>
<td>80.7</td>
<td>64.7</td>
<td>99.4</td>
<td>99.89</td>
<td>96.11</td>
<td>0.11</td>
<td>3.89</td>
</tr>
<tr>
<td>Noise</td>
<td>82.2</td>
<td>82</td>
<td>100</td>
<td>99.83</td>
<td>96.67</td>
<td>0.17</td>
<td>3.33</td>
</tr>
<tr>
<td>Amplitude</td>
<td>82.8</td>
<td>82.1</td>
<td>100</td>
<td>100</td>
<td>98.89</td>
<td>0</td>
<td>1.11</td>
</tr>
<tr>
<td>MP3(128kbps)</td>
<td>81.8</td>
<td>79.7</td>
<td>99.4</td>
<td>99.89</td>
<td>96.11</td>
<td>0.11</td>
<td>3.89</td>
</tr>
<tr>
<td>Lowpass Filtering(12kHz)</td>
<td>78.6</td>
<td>79.9</td>
<td>97.1</td>
<td>99.66</td>
<td>93.33</td>
<td>0.34</td>
<td>6.67</td>
</tr>
</tbody>
</table>

5. Conclusion

This paper proposed the hardware based watermarking algorithm for audio contents rights protection. It embedded the watermark on coefficient bits in the wavelet based frequency band as blind watermarking.

Consequently, by hardware implementation of proposed audio watermarking algorithm, it is possible to verify possibility of ownership protection commercialization, integration with actual applicable programs and efficiency followed by high level program development.

Implementation in the high level language such as the graphical language over the low level architecture demonstrates the balanced method in high level and low level programming. By this test environment, it is possible to easily modularize and expand. In addition, it is possible to prototype promptly, and the Blackfin processor used in this experiment is suitable for real time audio signal processing.

Audio watermarking technology implementation on hardware helps in integration of existing audio devices and audio watermarking chips and providing real time performance, as well as opens highly reliable, low power and low cost applications.

Spread Spectrum audio watermarking inserts data in the frequency range. By this feature, it provides robustly and imperceptibly watermarked signals.
6. Acknowledgement

This work was supported by a Research Grant of Pukyong National University (2013 year: C-D-2013-0552)

7. References