Music Information Acquisition, Preservation, and Retrieval (MUMT-611)

# Audio Watermarking Summary

Denis Lebel – 110125645 – denis.lebel@mail.mcgill.ca

## Introduction

Audio watermarking consists in embedding inaudible information into an audio signal. The technique was originally proposed as a way to counter music piracy. It is analogical to the paper technique used for money printing. The first audio watermarking techniques were directly inspired from previous research on image watermarking.

The remainder of this document compares watermarking and fingerprinting, describes the watermarking systems as well as their properties, and finally highlights some possible applications of watermarking.

## Watermarking versus Fingerprinting

Watermarking differs from fingerprinting in that the signal is altered when hiding information into it, whereas no modification, but only analysis, is performed on the signal when constructing the fingerprint. Watermarked signals have the advantage of being self-contained since they do not require any external repository to extract information from. However, the signals must be preprocessed in order to contain the watermark.

## Watermarking Systems

As mentioned in the previous section, a signal must be watermarked prior to its delivery. The watermark is usually constructed using a key. The reverse operation (watermark detection) also uses a key, which can be same or different than the original one used to in the construction. As in cryptography, if both the construction and detection operations are using the same key (symmetric), it is kept private (i.e., only the constructor and detector know the key). On the other hand, if a different key is used for detection, than that key is public (i.e., known of everybody). Note that in this case, the public key is usually derived from the secret key used during the construction process, but without inducing any hint about the secret key.

It is important to realize that even though there are some similarities with cryptography, watermarking is different since the audio data is always accessible, while an encrypted data is not readable unless decrypted first. Moreover, once decrypted the data is not protected anymore whereas the watermark is permanent.

Any devices or systems interacting with the signal must check for the presence of a watermark before proceeding with further operations. Thus, a detection mechanism is required to perform this task.

## Properties

When designing a watermarking system, some general properties must be taken into account as described in (Gomes et al. 2003).

- **Inaudibility**: No sound quality degradation.
- **Robustness**: Resistance to any signal transformation.
- **Capacity**: Watermark bit rate.
- **Reliability**: Error rate during detection.
- **Low Complexity**: Computational costs the system (lower = better).

These properties are interrelated, thus a tradeoff needs to be made in order to meet the requirements. For example, a system designed for mobile devices requires a lower complexity, which may in return provide less robustness.

## Psychoacoustic Model

Watermarking uses psychoacoustic models in order to ensure that it is not perceivable. In the frequency domain, for example, masking thresholds are used to calculate the amount of data that can be added in each frequency bin without being audible. It is exactly the same concept used in lossy audio compression algorithms (e.g., AAC).

## Techniques

### Spread-spectrum

The idea behind the spread-spectrum technique is to spread a pseudo-random sequence across the time-domain or transform signal. The sequence is generated using a secret key. The watermark is embedded in the signal as a modulation of the pseudo-random sequence, and of course scaled according to a psychoacoustic model (Figure 1).

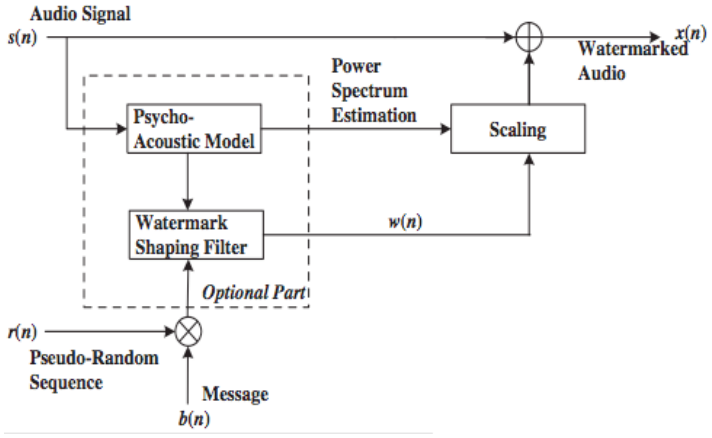


**Figure 1: Spread-spectrum scheme (Kim et al. 2004)**

**Replica**
This method uses the signal itself to create the watermark. One common technique is called "echo hiding", which consists in introducing echo in the time-domain. The watermark is embedded in the signal by echoing the original signal with two different delay lengths. The bit value encoded depends on the delay length used.

**Self-Marking**
This technique consists in embedding a special signal into the audio. A trivial example is to introduce a peak in the frequency domain.

## Applications

As previously mentioned, audio watermarking was initially introduced as a copyrights protection mechanism. Two examples of this are to enforce usage policy of audio content or to provide a proof of ownership. However, in order for a watermarking system to be secure, it would require all audio devices to conform to the technology. The other major problem is that if one has access to the detector algorithm, then the whole system can be reversed engineered, which is analogous to what happened with the DVD as recalled Craver et al. (2001).

Forensic watermarking is another application in which the watermark needs to be really fragile, which contrasts with copyrights protection. The watermark becomes no longer detectable if the content is altered.

Finally, one application that could be interesting, but has yet to be extensively studied, is the information hiding to add value to the distributed content. It could even be used to embed annotation data.

## Conclusion

Audio watermarking could potentially be useful since it is self-contained. However, the technique by itself does not have much hope if used for copyrights protection. Thus, watermarking should really be considered from a different perspective.

## References

Gomes, L., P. Cano, E. Gomez, M. Bonnet, and E. Battle. 2003. Audio watermarking and fingerprinting: For which applications? *Journal of New Music Research* 32 (1): 65–81.

Craver, S., M. Wu, and B. Liu. 2001. What can we reasonably expect from watermarks? *IEEE Workshop on the Applications of Signal Processing to Audio and Acoustics*. 223–6.

Kim, H, Y. Choi, J. Seok, and J. Hong. 2004. Audio watermarking techniques. In *Intelligent watermarking techniques,* edited by J. Pan, H. Huang, and L. Jain, 185–219. River Edge, N.J.: World Scientific.