

THE SENSE AND NONSENSE OF WATERMARKING

Ton Kalker

Philips Research Eindhoven
ton.kalker@ieee.org

SUMMARY

The number of ways in which we may obtain audio-visual data has enormously increased in recent history. We have gone from live performances, to analog physical carriers, to digital physical carriers to non-physical distribution. However, the increased ease of distribution as well as rendering of audio-visual data has not only positive aspects, but negative aspects as well. In particular, the payment component of multimedia delivery over online networks has some serious problems and flaws (example: Napster, KaZaa).

It has been proposed that digital watermarking is a good solution to reduce the amount of illegal copying and the abundant illegal distribution of multimedia assets. The basic philosophy in using a digital watermark is very simple: 'a watermark is imperceptible and robust to degradations that preserve perceptual quality; therefore it can serve as a non-erasable flag to indicate that copying and redistribution are restricted or even forbidden'. The unspoken assumption here is that imperceptibility and robustness naturally lead to security. Very often watermarking has been seen as the digital-signal-processing equivalent of cryptography. This is also reflected in literature where for example Kerckhoffs' principle (well known in cryptography) is often extended to watermarking.

In this presentation we will first argue that there is a fundamental difference between cryptography and digital watermarking. A first fundamental difference is the bit-sensitivity of cryptographic solutions whereas digital watermarking solutions have a more continuous behavior. This has important implications for the amount of effort needed to re-engineer a cryptographic solution versus a watermarking solution. A second fundamental difference is the fact that cryptographic solutions are active and watermarking solutions are passive. These differences and their implications will be highlighted. In particular we will conclude that the simple philosophy of the previous paragraph needs a much more thorough elaboration, and cannot simply be applied 'as is'.

In the second part of the talk we will take a more positive look at digital watermarking and show how it can be successfully applied to a number of applications. We do this by re-examining the basic properties of digital watermarks and by showing how these basic properties can serve a real need. Among the opportunities we will discuss are broadcast monitoring and forensic tracking. With respect to the latter we will also argue that digital watermarking is only a small part in the total chain, and that a total system requires both other signal processing tools (e.g. robust hashing and coding) as well as cryptographic components.

We conclude by looking into the future and trying to predict where digital watermarking will go, both in an academic as well as in a business sense.