© WATERMARK: CLOSING THE ANALOG HOLE

*Eric DIEHL, Teddy FURON**
THOMSON multimedia RD France
1 Avenue Belle Fontaine, 35510 CESSON SEVIGNE, France
**TEMICS / INRIA*
Campus universitaire de Beaulieu
35000 RENNES, FRANCE
Email: eric.diehl@thomson.net; teddy.furon@irisa.fr

Abstract

The © watermark offers a more robust method to close the analog hole piracy. It has a simpler trust model than current solutions. It offers better resistance to malicious attacks.

Key Words

Copy protection, watermark, analog input

Introduction

This paper is about copy protection and watermarking. It presents a way to close the analog hole through a new concept so called the © watermark. It compares this new concept with the current watermarked-based approach.

The analog hole problem

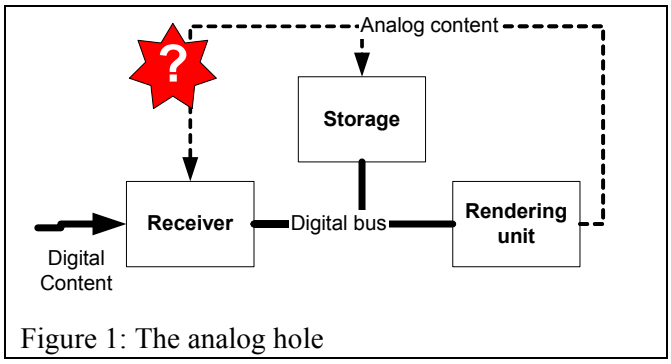

Figure 1: The analog hole

The dawn of digital world also boosted piracy of digital content. The current response is scrambling content. This answer is suitable as long as content remains digital. Unfortunately, the weakest link in the delivery chain is the analog link. Video has to be rendered on a display. Audio has to be played through loud speakers. Pirates, as dishonest users, can play the content, record these analog signals, digitise them, and distribute the files. We call this threat the analog hole. Figure 1 illustrates the problem.

Using watermark

Watermarking is considered as a promising technology to close the analog hole. A watermark is a signal added in the video pixels. A human visual system ensures the watermark embedding is non-perceptible. This signal is a carrier transmitting hidden data. It is robust if devices retrieve the hidden data from content that has undergone some video processing like compression, scaling, and colour adjustment for instance. Thus, a robust watermarking survives through the analog path.

Typical approach

Having in hand such technology, designers must specify its use within a copy protection system. In the current approach, the embedded data describe the copy conditions of digital content. For instance, it may carry one of the following three states: “Copy Never”, “Copy Once”, “Copy no more”. Not watermarked pieces of content are considered as “Copy free”. Therefore, receivers should detect these data, and spot illegal content re-entering the digital domain. If the content is legal, then receiving device scrambles analog content to provide protection within the digital network.

The © watermark approach

The new concept of © watermark combines strong watermarking with content scrambling. As in the previous approach, scrambling protects digital content within the home network. Before rendering, the device checks two conditions: is the digital

content scrambled? Is the digital content © watermarked?

	Scrambled	Not scrambled
Watermark	Legal content	Illegal content
No watermark	Legal content *(not protected against analog hole)*	Free content

Previous table defines the behaviour of the rendering device, which does not play illegal content.

Comparing the two approaches

We compare two parameters: the associated trust model, and the resistance to malicious attacks.

Trust model

In the typical approach, watermark detection occurs at reception. This approach makes the following trust assumptions:

- H1: The rendering device is compliant.
- H2: The rendering device receives only content from compliant receivers or compliant storage units.
- H3: Analog inputs of compliant receivers and storage implement watermark detection.
- H4: Analog content can only enter the digital network through the analog input of a compliant device.

H1, and H2 are the typical trust assumptions for non end-to-end protection schemes. Every element of the chain has to be compliant. H3 is the basis of this watermark protection scheme. H4 is mandatory; the rendering unit assumes that its contents are legal. Thus, it expects that content from analog source passed the watermark detection.

Unfortunately, assumption H4 is wrong. A pirate may digitise analog content through a non-compliant device, then import the now digital content into the network, for instance through a recordable media, or network hard disk.

With © watermark, detection occurs at rendering point rather than at reception. Thus, the system makes the following trust assumptions:

- H1': The rendering device is compliant.

H1' means that it implements the concept of © watermark. Most significantly, the © watermark needs no hypothesis, such as H4, on the content to render. If the pirate applies the attack described previously, he will get a clear digital content with a © watermark. Thus, the rendering device will spot it as illegal.

The © watermark concept reduces the number of security requirements. Therefore, the second trust model is simpler and stronger.

Malicious attacks

Interestingly, the security levels of the two approaches are different even if the techniques use the same watermarking technology.

In the first approach, watermark's payload is meaningful. Impairing the payload modifies the behaviour of the system. In the second approach, the © watermark has no payload. Theoretical studies have shown a trade-off between non-perceptibility, payload and robustness. Thus, reducing payload to the minimum guarantees a better robustness. It also reduces the complexity of the decoders.

Moreover, the state of content is changing in the network. For instance, legal duplication changes "Copy Once" in "Copy no more". In the first approach, storage units have thus a complex watermark embedder to modify this state. Yet, this is a security flaw as pirates can hack the watermarking technique by comparing content before and after the watermark insertion. In the second approach, content producers watermark and encrypt the videos once for all as an end-to-end protection.

Conclusion

The problem of the analog hole is an important issue in the copy protection battlefield. If not well closed, it may jeopardize all the digital copy protection schemes.

We presented a new approach entangling the advantages of scrambling and watermark. Locating the watermark detection at the end of the chain, rather than at the beginning, drastically reduces the number of trust assumptions. Thus, the trust model is stronger. Furthermore, using a null payload, it increases the robustness against malicious attacks to wash the watermark.