

Watermarking takes the plunge

An undetectable spy

The principle of this digital marking technology is to add to video or audio content an invisible, inaudible trace that can be subsequently identified. One of the associated functions is to fight against piracy: the technology can identify the source the content was copied from, a vital feature for major studios and other content providers.

Note that one of the main sources of piracy for motion picture studios is the duplication of films made directly in theaters using digital cameras. This content is then distributed in parallel on DVDs or over the Internet. In this context, watermarking can track down the movie theater responsible for the leak, as it adds a specific mark for each theater.

Until now, Watermarking solutions were mainly in 'Business to Business' solutions, i.e. for protecting exchanges between companies. Today they are becoming widespread.

Digital terminals: a new place to hide

The new technologies in consumer electronic devices over the past few years have permitted to make recordings and even to distribute them, either by suitable outputs (such as USB) or through built-in burners. While Conditional Access technologies are particularly well suited to protecting live content, they are less effective for recorded content, and new DRM solutions are being implemented.

More than simple DRM protection systems which prevent copying, for example, additional solutions use watermarking technologies in digital terminals. The basic idea is to insert a

mark in the decoded content on the fly and in real-time. All the possible outputs of the digital terminal (either analog or digital, including storage devices) will carry content with the added watermark. This mark unambiguously identifies the serial number of the terminal or of the subscriber's smart card.

If the marked content is later found on a Web site or in parallel DVD markets, these tools make it possible to find the watermark and track down the source of the leak in order to implement legal action if necessary.

On your marks!

Thomson Security, Cinea (part of the Dolby group) and Philips presented

Security's Watermarking. In fact the demonstration we saw on the Thomson Security booth used the solution integrated with Viaccess. In this context, an ID in the subscriber's smart card is marked in the content. Logically, Verimatrix directly includes its Watermarking solution in its own Conditional Access solution.

To summarize, watermarking – which can also be used without Conditional Access for unscrambled content unprotected by Conditional Access – is showing up everywhere.

OK, but what about performance?

It is difficult to test the robustness and reliability of solutions presented at a show. Here are some of the major

Watermarking methods

Steganography, used extensively for watermarking, is a technique that conceals a message in a document with visibly innocuous content, so that the message remains secret.

Several historical anecdotes illustrate this technique, such as invisible ink. During the 4th century BC, Herodotus wrote that in the court of Persia, a

certain Histiaeus wanted to communicate with his son-in-law, the tyrant Aritagoras of Milletus. He chose a devoted servant, shaved his head, and tattooed a message on his scalp. Then he waited until the servant's hair grew back before sending him on his way with instructions to shave after he was in Aristogas' presence.

their Watermarking solutions integrated directly in digital terminal chipsets. The Thomson solutions is currently integrated with ST, while Philips' is included in ST, Broadcom, and Texas Instruments chips. Verimatrix includes its proprietary technology in its chipsets. But what about Conditional Access suppliers?

Viaccess and Irdeto both announced the integration of their conditional access solution using Thomson

questions you should ask when evaluating a Watermarking solution:

- Is the mark truly invisible or inaudible?
- Is the marking algorithm sufficiently secure?
- Might the watermark be removed from the content through successive processing steps?

These questions let you compare the integrated solutions used.