

The oncoming wave of digital watermarking

As digital pirates become more sophisticated, broadcasters need more sophisticated identification mechanisms. Global piracy is estimated to cost Hollywood almost \$4bn a year through the recording of films with a camcorder. In response, the Digital Cinema Initiatives was created, which mandated the development and use of forensic anti-piracy technology. Crucially, watermarking survives capture with an HD camera. The so-called analogue hole is the major advantage that watermarking has over all other security techniques.

Originally introduced to the professional film industry, the technology has subsequently been expanded to support marking video content streams down to specific consumer devices, from set-top boxes (STBs) to portable video devices to mobile phones. The experience - and success - of watermarking in this area has led to the technology being considered in the consumer domain and there is a great deal of attention being placed on watermarking for payTV.

While CA controls access and DRM enforces rights, watermarking can provide indelible evidence of where rights have been abused, and beyond that an audit trail of the content's history. Its purpose is to act as a deterrent and as a forensic tracking tool. Forensic watermarking is the placing of an imperceptible ID number (known as a payload), similar to a bar code, into a unique video stream. Watermarking tracks where, when and to what device content is delivered, regardless of network, device or video format. In the event of theft, this approach enhances the possibility of tracking piracy down to the individual. This playback makes watermarking a complement beyond the DRM envelope and a value-add to traditional CA systems.

Unlike other types of watermarking that have different attributes, forensic

A number of drivers are leading payTV providers to deploy forensic watermarking, but the most interesting business models are slowly emerging, says Goran Nastic

watermarking is very specifically about tracking back to the original copy, and this form of watermarking will be the most commonly used form for video content. A frequently cited rationale is that watermarks keep 'honest people honest'.

Watermarking technology has been available for 20 years in the professional environment. While there are only one or two commercially announced watermarking deployments by payTV providers - it is in trials and proof of concept stage - two key

"Belgacom set a precedent by recently announcing that its service has been granted the same release window for VoD as for DVDs."

drivers exist that will help proliferate its use: the rise of HD content and video-on-demand (VoD).

Watermarking is being looked at as a solution to help payTV operators in their quest for early release windows for VoD content. Indications from analysts and studios point to watermarking enabling simultaneous releases between VoD and DVDs. Belgacom set a precedent by recently announcing that its service, which is protected by Verimatrix' software, has been granted the same release window for VoD as for DVD titles.

For operators, this would open a lucrative new revenue opportunity and potentially stands to provide a real boost to VoD usage. VoD operators have an opportunity to gain carriage licences to high value

content sooner, cheaper and with wider rights for resale. The use of watermarking doesn't necessarily guarantee any deal for early access content, but as Alex Terpstra, CEO of watermarking vendor Philips Content ID, puts it, "By embracing watermarking proactively, you will at least have a chance, as opposed to no chance."

While the DVD market for studios is more valuable than even the theatre release, Robert Payne, VP of sales for EMEA at Verimatrix, suggests the technology can

even be used as a negotiating tool for lower prices for early release content. An added incentive for studios compared to the DVD model is that they could save on the production costs (namely packaging and distribution) with digital VoD. There are even suggestions that VoD windows could be as early as theatrical release.

This makes watermarking appealing to all operators - cable, satellite, IPTV and terrestrial - and vendors in this space claim equal levels of interest from all of them. "It's gone from being an edgy new idea to being very substantial to the mainstream operators," says Laurence Roth, VP of marketing and business development at Cinea, a Dolby subsidiary, who adds that large Tier 1s are coming to the company asking about its Running Marks solution.



Verimatrix's VideoMark technology

Cinea is unique in that it marks content in the compressed domain, with support for MPEG-2 and H.264 codecs. The company says there are no trade-offs in terms of security or robustness found in this approach. Indeed, it says it has gained traction specifically because it operates in the compressed domain. Cinea also claims its architecture and lightweight inserters are extremely simple to integrate. This dependence on codecs, some argue however, makes it more difficult to future-proof in case of new compression standards or resolution formats.

There were various watermarking demonstrations at IBC this year, and everyone from operators to CA vendors to silicon providers has some interest. For this reason, broad partnerships are continuing to evolve between watermarking and CA players, who want to make their solutions as appealing as possible to all operators. So, for example, while Irdeto has integrated with Phillips and Thomson, it says the door is still open for other watermarking vendors. For its part, Thomson has announced integration with all the major CA vendors, including Irdeto, Viaccess, Nagravision, Conax and Widevine. Moreover, these vendors are integrating with the major IC vendors, including Texas Instruments, Broadcom, STMicro and Conexant.

TVN Entertainment, which reportedly watermarks all its video content (about 3,500 hours a month) for distribution to most major MSOs and telcos in North America, performed tests where watermarked video was MPEG-2 compressed at 3.75 Mbps, projected onto a wall, camcordered directly from that wall, and

re-encoded to H.264, at a bit rate of 500 kbps. The detector was able to recover the watermark from this video in all instances within the first minute of the captured file. In this case, the results were carried out on systems from Thomson, Cinea and Phillips.

Fundamentally, marks must be invisible to the human eye, particularly in HD content, and they must resist intentional and unintentional attempts to delete them. All watermarking vendors claim they are resistant to all known forms of attack, including transcoding, recompression, resolution changes, scaling, cropping, rotating and so on.

Of course, there are limits, but it must be taken into account to what video quality level it is useful to have a watermark system detecting the payload. Most vendors claim that their watermarks are so enduring that the degree of degradation of the original asset necessary to remove the watermark would render the asset unusable for commercial purposes. The value of the content may erode to such an extent that it doesn't necessarily make sense for the watermark to be present any more.

This raises the issue of whether watermarking will make its way into SD content. The general consensus is that there will never be a commercial incentive for watermarking SD content, although operationally it may be easier for operators to watermark all content.

Nevertheless, one potential application for watermarking SD content is the illicit redistribution of the TV signal on a continuous basis in emerging markets, notes Phillips' Terstra. He cites examples of pirates connecting the output of an STB to a local network and feeding hundreds of people illegally. This can be tackled by watermarking and it is in the interest of the payTV provider to do so.

Headends vs STBs

Watermarks can be inserted at different stages and then read at various points of the distribution chain. In payTV distribution, there are two methods of watermarking commonly used. The first is server-side watermarking, whereby a watermark is

incorporated at the point of ingest into the playout system. Here, part of the encryption process in the VoD system incorporates the watermark, and all assets are watermarked all the time. The benefit of this approach is that it doesn't affect legacy devices, which makes for a more straightforward and less costly implementation.

The disadvantage is that the watermark is not unique as it only identifies the broadcaster/operator, making it limited in forensic detection terms because it only identifies the operator responsible for the loss of the content. "This doesn't give operators an incentive to watermark content because the only thing they will establish is that they have a leak," argues Payne.

Watermarking technology can also be placed down at the device level (such as an STB), a process also known as session-based watermarking. In this case, the watermark uniquely identifies the playout device and therefore the individual subscriber that leaked the content. While this approach provides an effective tracking mechanism for tracking the time and place of the theft, it means that watermarking systems have to be integrated into every STB (or PC).

Modifications include utilising secure chip memory on the latest STBs, at which level most vendors typically integrate. According to Payne, "The upside of a session-based watermark is that you get time, date, asset, transaction and subscriber information all incorporated into the security signage, making it ideal for prosecutorial and forensic tracking."

Pascal Marie, Thomson's NexGuard product line manager, further argues that the replacement of legacy boxes with next-generation STBs provides a good rationale for watermarking. "At some point, there is a decision to be made about starting to implement watermarking, and certainly the introduction of new generation of STBs able to handle HD is an interesting start point," he points out.

Darren Granger, chief technical engineer at Pace Micro, which expects to integrate watermarking into its products next year, says that the effect of watermarking on the

“Watermarking could legalise the P2P model through the insertion of targeted adverts in the watermark.”

performance of the STB is minimal, as it is not the main processor that is embedding the watermarking but the video decoder. “The only side effect is that the video decode process takes slightly longer, this can add a one frame delay on some silicon. If watermarking is maintained through trick modes then it is possible that smooth trick modes will not be run up to their current rate,” he says.

Granger adds that the answer to which boxes can be upgraded on the field depends on the watermarking system to be ported. Generally, it would require a reprogrammable video core, which most modern STB chips have, and willingness for the IC vendor to update it.

New business models

Arguably the most interesting application of watermarking is in enabling new business models around advertising revenue generation and peer-to-peer (P2P) distribution. It is an application where watermarks are used as a personal identifier embedded in content in P2P networks where they are used to trigger targeted ad insertion. In effect, watermarking could legalise the P2P model.

Widevine is the main proponent of this approach, arguing that the way its Mensor solution encrypts and watermarks content enables advertising to remain part of the streamed content and makes it trackable. “This creates a business model to distribute content for free where the content owner is generating revenue from the number of eyeballs that see the ads, which provides the consumption verification and tracking required to validate the numbers that are provided to advertisers,” says Barbara Leavitt, director of marketing at Widevine. This also supports legalisation of a P2P model since content owners are getting revenue through advertising.

Additionally, Leavitt envisages new models emerge where a user gets credit for

passing on content because information in the watermark can identify and track who has viewed content and when. A video player within a P2P client could read the Mensor watermark and disable the playback - or direct the user to an e-commerce site to buy the rights to view the content - depending upon business rules indelibly marked in the content.

According to Cinea's Roth, ease of detection and robustness are the key characteristics here, since without it the user community will most likely remove the watermark in order to access the content without the ads, and if the watermark is not quick to detect, the user will not wait for the content to play.

Because watermarking is less obtrusive than CA or DRM, it is designed to address piracy in a positive way. Andy Nobbs, president of Teletrax, a JV between Philips and Medialink, which uses watermarking as part of its global broadcast monitoring network for content producers, says broadcasters can learn from the experience of the music industry, which unsuccessfully tried to regulate online content.

“If you can provide content owners with a mechanism whereby they can engage with consumers and allow them to easily access and enjoy content but know what has happened, then you can monetise it in a way that's consumer friendly. Show me a DRM system that is liked by consumers. It's antithetical and counterintuitive to the digital economy in general,” he adds.

Eliminating false positives

The watermark detection process is mainly about statistics and error correction management. All watermarking technology implements error correcting coding (ECC) algorithms to prevent the occurrence of false positives. ECC takes the application message, which is essentially the serial number, and applies mathematical algorithms, so when they are retrieved there is a high probability that the number is the same as in the content. While ECC is a key mechanism to overcome false positives, other techniques also exist that have the ability to use the functionality or parameters of the watermark to address false positives. ECC and its ilk aren't fool-proof, but all watermarking vendors claim that the occurrence of false positives within their solutions is virtually zero.

These sentiments are echoed to a degree by Mike McGuire, research VP of media at Gartner. “We think equally important, over time, are systems that use a watermark as an identifier to enable a level of viral sharing. This will have some interesting long-term effects on the business models, some of which can be ad supported and others involving for-pay distribution.

“The industry has to get much more creative about establishing alternate business models, whether they are ad supported or just better transaction systems. Unless digital payment systems improve, all the watermarking in the world isn't going to be of much benefit.

“Our recommendation is look at the tag to enable active content dialogue. That persistent watermark can essentially turn a piece of ‘static’ content into a tag, which becomes the identifier to send updated information by the service provider that may be of interest to the consumer. What we see, especially with the growth of IPTV, is that these kinds of models for distributing content are gaining some traction,” adds McGuire.

Where does this brave new world leave traditional CA/DRM? McGuire sees CA/DRM providers moving towards taking their technology and applying it to delivering new content experience models. “We're not saying do away with DRM. Rather, the focus needs to shift from developing and deploying hard-locked encrypted DRM to deploying systems that track/account for consumption and do it in such a way that multiple business models can evolve.”

Expect to hear a lot more on this front in the coming months and years. **CSI**