# APPLYING DIGITAL WATERMARKING TO HOME ENTERTAINMENT CONTENT DELIVERY NETWORKS

Reza Rassool, Chief Engineer
Widevine Technologies Inc.

*Abstract*

*Watermarking technology, answering TV industry requirements, (1) has emerged in trials over the last few years. While the initial deployment focus has been largely on future digital cinema applications (2), there are significant challenges of scalability, performance, and economy in adapting the same technology to today's content delivery networks (CDN) to the home. This paper, drawing from RFI (3) responses for candidate technology for the Widevine 'Mensor™' (4) digital forensic system, discusses the compromises necessary to engineer an economical watermarking solution for home entertainment.*

## INTRODUCTION

Anti-piracy, digital rights management and copy protection technology have long been the subject of scientific endeavor in the entertainment industry. Specifically the quest for an imperceptible means to deter and track unentitled usage of content has resulted in technology called *watermarking*.

Since 2004 the content owners have increasingly included the term 'watermarking' in their questionnaires to service owners who seek content. While this language has not yet translated into specific requirements in carriage contracts, they do give service operators and manufacturers notice of impending conditions for obtaining content in the future.

In 2005, Widevine Technologies Inc., a supplier of security solutions to the entertainment industry issued a request for information (RFI) to core technology suppliers for watermarking components to be included in its Mensor digital forensic product line. This paper charts the technical inquiry to derive a set of requirements for watermarking for home entertainments networks. It draws from the RFI responses while respecting the confidentiality of the respondents.

## REQUIREMENTS

Digital Cinema Initiatives, LLC (DCI) was created in March 2002, as a joint venture of Disney, Fox, MGM, Paramount, Sony Pictures Entertainment, Universal and Warner Bros. Studios. DCI's primary purpose is to establish and document voluntary specifications for an open architecture for digital cinema that ensures a uniform and high level of technical performance, reliability, and quality control. The Digital Cinema System Specification V1.0 includes requirements for the watermarking of content. In September 2002 the European Broadcasting Union (EBU) reported (1) on the trials of watermarking technology to meet the needs of digital television. The EBU differentiates the watermarking requirements of the W1 (contribution), W2 (distribution) and W3 (consumption) segments of the content pipeline.

Of the two sets of requirements, the digital cinema business appeared to capture the immediate focus of technology suppliers. Even the emphasis of the EBU was on the W1 and W2 segments of the content

pipeline. Now, as IPTV emerges as a significant market for entertainment content, technology suppliers are having to modify their strategies concerning forensics as, they either retool or design anew solutions for W3 – watermarking content right to the home and beyond.

Why Extend Watermarking to the Home?

The commercial rationale for deploying digital forensics to the home entertainment network can be simply stated – It may become a contractual pre-requisite for obtaining content.

1) Theft deterrence

Watermarking is proposed as a theft deterrent – to keep honest people honest. In this respect users should be made aware of the watermark's existence. Ironically the most carefully engineered quality of a watermark's invisibility detracts from its deterrent effect. To augment the deterrent effect it is important to use other means to alert the user that the content they are accessing is watermarked with a payload that uniquely identifies their client device and the time of access. This can include a visible mark or a warning introduction to the content.

2) Carriage contract questionnaires

Without divulging confidentiality it can be said that the studios have increasingly employed language in questionnaires ranging from a general query,

> "Has your company deployed any forensic watermarking (invisible) technology? If so, please describe in detail."

to very specific questions regarding the watermarking capabilities of service operator's network.

> "Is the STB capable of session based watermarking for high value content?
> 1. Please identify the watermarking technology used and the payload.
> 2. Please describe the forensic marking process.
> 3. Please describe the forensic marking detection and recovery process.
> 4. Please describe the robustness of the watermark in terms of survivability to obscuration, down rez, or overmarking."

3) Tracking

Watermarking is also useful in providing evidence of theft in criminal proceedings. The Mensor technology has already proven itself in court. Twenty-eight of the world's largest entertainment companies brought the lawsuit against the makers of the Morpheus, Grokster, and KaZaA software products. Evidence for the plaintiff was provided by early Mensor technology. The case was decided on June 27, 2005 in favor of the plaintiff. [7]

4) Leak detection

Watermarking is further used to detect breaches of security in a content delivery network. Leak location in a multi-node CDN requires that the watermarking scheme supports:

- embedding at multiple nodes
- multiple overlapping marks or mark replacement

5) Security renewal targeting

Through the extraction of the payload from pirated content the service operator, aggregator, or content owner is able to identify the node of the CDN from which the content was obtained. This allows for the targeted renewal of security in the

conditional access systems of the CDN. The cost of security renewal can be prohibitive without such targeting.

6) Copy protection

Watermarking has also been promoted as part of a copy protection system. This scheme, which has had limited success, requires that a client device is capable of reading watermarks and respecting the copy control information contained therein.

7) Content tracking

Watermarking additionally provides a means to embed metadata into content that will survive numerous transport mechanisms. This usage of watermarking is used to monitor and audit the delivery of paid content such as advertising. (5)

8) QoS optimization

A hidden bonus for service operators is the promise of using the feedback of extracted metadata from the edge of a CDN to optimize the serving of content. VOD content is transmitted by an aggregator, such as TVN, to hundreds of nationally distributed VOD servers. Local usage data could be used to tune the forward transmission of the most popular titles in a particular area.

9) Enabling new business models

As peer to peer files sharing network companies scramble to legalize – watermarking technology offers a solution. One can imagine that a P2P player could extract and respect an embedded payload, and then allow the user to purchase an entitlement for legitimate access to the content.

## ENGINEERING CHALLENGE

The challenge for engineers is to glean rational requirements from the esoteric messages from the industry and sparse data points in related fields. Specifically, the challenge facing the author's colleagues was to design a digital forensic system that would be economically and computationally appropriate for deployment in content owner/aggregator facilities, operator head-ends, and customer devices.

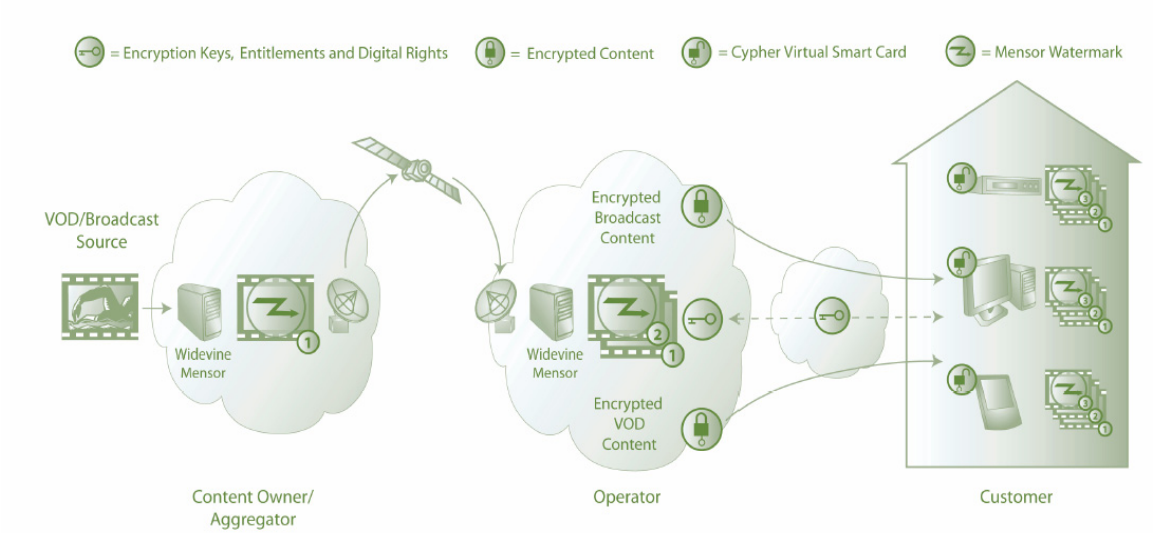


Figure 1. Watermarking applied to a multi-stage content delivery network

Figure 1 shows a multistage content delivery network. The content originates with a content owner or content aggregator. The content is transmitted to a service operator. The diagram shows a satellite transmission, however, other means are also used. The service operator serves both broadcast and VOD content to numerous customers.

Build or Buy

There are numerous attractions to originating core technology specifically tuned for an application; however engineers rarely have that luxury. In the case of watermarking there exists a wealth of prior art and core technology that has already gained industry acceptance. In the security field there is a distinct disadvantage to 'home grown' algorithms. Specifically, cryptographic products with industry standard algorithms such as AES have greater credibility than those with proprietary algorithms. Another factor particular to watermarking is the reality that Digimarc Corporation has a strong patent portfolio with far reaching claims. These factors encouraged us to adopt the course of licensing and integrating 3rd party watermarking components into a design for a digital forensics system.

Adapting Existing Technology

It is clearly unfeasible to place a $20,000 watermarking engine, designed for post production applications; into a sub $100 set top box for session based watermarking. The technical challenges include:

- scaling the head-end embedder to handle hundreds of streams
- implementing watermarking algorithms within the CPU budget of a set top box processor
- integrating watermarking into a security framework.

In order to understand how to adapt the existing algorithms, it is necessary to formulate a model to quantify the variables by which we can judge a watermarking scheme.

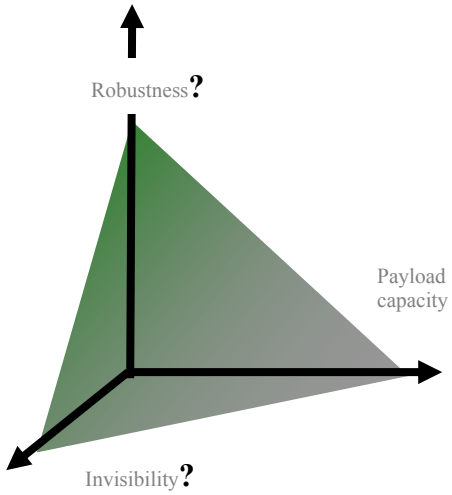


Figure 2. Watermarking dimensions

The concept in the figure above is often expressed but very rarely substantiated. Of these three dimensions only payload capacity is quantified.

Invisibility is a Pre-requisite

Even though the EBU requirements state:

"Note that the invisibility of the watermark, which is a typical subjective consideration, is different for W1 (at contribution level) and W2 (at contribution end-user level)." [1]

The result of analysis of watermarking algorithms shows that it is not practical to vary the invisibility of the watermarking algorithm. The method of spread spectrum coding of a signal through selective DCT modifications, exhibits a cliff effect with regards to invisibility (6). The mark is either invisible or obviously visible.

Through interviews with Hollywood content owners we found little acceptance for watermarks that were anything but invisible.

By accepting invisibility as a prerequisite, we now have the variables of payload capacity and robustness to tune to arrive at an optimally engineered solution.

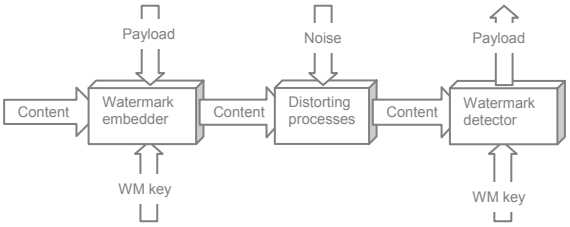


Figure 3. Watermarking dataflow

The figure above shows the typical end-to-end dataflow for watermarking. The watermarking embedder uses a watermarking key, WM key, to securely embed a payload into the content. The payload is embedded into a segment of content define in time as the watermarking minimum segment (WMS) (1).

We define here the notion of watermarking strength, $S_w$ in terms of signal to noise ratio.

If the signal rate is $R_s$ and the payload rate is $R_p$. Then with a payload size of $P$ bits:

$$R_p = \frac{P}{WMS} \quad \textbf{(b/s)} \qquad \text{Equation 1}$$

$$S_w = \log\left(\frac{R_s}{R_p}\right) \qquad \text{Equation 2}$$

Additionally in the figure we see that a watermark's robustness can be defined in terms of the watermark to survive noise added into a distorting process. Robustness is not easily quantifiable. Among enumerations of various transformations or signal distortions to which the watermarked content should be subjected, the industry requirements commonly define robustness in terms of the lowest compressed rate, $R_c$, from which the payload must be recovered.

We focus on this quantification of robustness and then as in equation 2 express the maximum distortion, $D_{max}$, in terms of a signal, $R_s$ to noise, $R_n$, ratio.

$$D_{\max} = \log\left(\frac{R_s}{R_n}\right) \qquad \text{Equation 3}$$

Now we can go further and express robustness, R, as the ratio of watermarking strength and maximum distortion.

$$R = \frac{D_{\max}}{S_w} \qquad \text{Equation 4}$$

Restated, this becomes

$$R = \frac{\log\left(\frac{R_s}{R_n}\right)}{\log\left(\frac{R_s}{R_p}\right)} = \log_{Rp} R_n$$

Or

$$R_p{}^R = R_n \qquad \text{Equation 5}$$

This eliminates the content signal rate from the relationship. R is a characteristic of a specific watermarking algorithm. Equation 5 indicates that for a given engineered robustness, R, as the payload size or WMS is increased there is a logarithmic in Rn, the lowest compression rate from which the watermark can still be extracted.

Robustness is increased by redundantly inserting the mark into the content which entails increased computational expense.

| Requirements | DCI System Spec V1.0 | EBU W1 | EBU W2 |
|---|---|---|---|
| WMS | 5 mins | 1 sec | 5 sec |
| Payload size | 35bits | 64bits | 64 bits |
| Signal data rate | JPEG 2000 @250Mb/s | SDI @270Mb/s | MPEG-2 @ 8Mb/s |
| Robust to compression rate | 1.1Mb/s | 2Mb/s | 2Mb/s |

Table 1. Quantifiable EBU and DCI requirements

The DCI and EBU requirements are shown in Table 1. From these we can calculate values of robustness.

The head-end watermarking embedder, Mensor Server embeds a payload of 21 bits while the Mensor Client embeds a payload of 64 bits in session based watermarks. The following table shows the resulting robustness. Note: The results have been scaled using content bit rate in Mb/s and payload bit rate in bit / second.

| | Robustness |
|---|---|
| EBU W1 | 0.322 |
| EBU W2 | 0.055 |
| DCI | 0.240 |
| Mensor Server | 0.041 |
| Mensor Client | 0.039 |

Table 2. Robustness

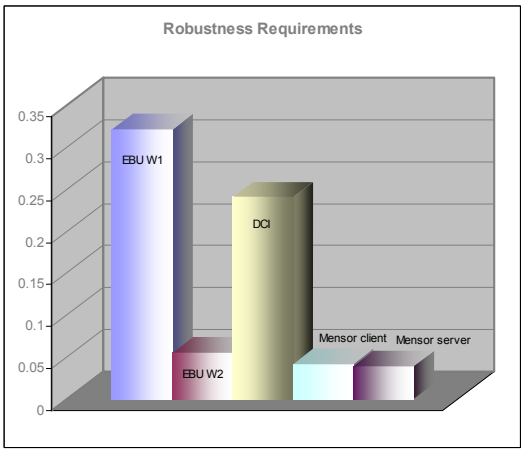


Figure 4. Robustness requirements of various watermarking systems

## CONCLUSION

Robustness can be quantified and related to payload bit rate by

$$R_p^{\ R} = R_n$$

In engineering a cost effective watermarking solution for home entertainment, we utilize savings in reducing robustness. We see that EBU W1 and DCI require high robustness while EBU W2 and Mensor call for an order of magnitude lower robustness. Reduction is robustness translated into a reduction in cost and has enabled us to arrive at a cost effective home entertainment watermarking solution.

## BIBLIOGRAPHY

[1] Choosing A Watermarking System For Digital Television - The Technology And The Compromises
L. Cheveau, European Broadcasting Union, Switzerland, IBC 2002 Conference Proceedings

[2] DCI Digital Cinema System Specification v1.0a

[3] Content Watermarking System Request For Information (RFI) V1.1, Widevine Technologies Inc.

[4] Antipiracy - Trends And Technology (A Report From The Front)
R.P. Rassool, Widevine Technologies Inc., IBC 2002 Conference Proceedings

[5] Teletrax™ Technical Specification, Philips.

[6] Robust Hash Functions for Digital Watermarking, Jiri Fridrich and Miroslav Goljan, Center for Intelligent Systems, SUNY Binghamton

[7] MGM Studios Inc., et al v. Grokster, Ltd., No. 04-480 on the Supreme Court's docket, June 27, 2005.