

# Ongoing Innovation in Digital Watermarking

➔ **Rajan Samtani**, *Digimarc Corp.*



**Watermarking-based applications can help content owners balance business requirements with consumer choice.**

**D**igital watermarking is the process by which digital information—referred to as a “payload”—is embedded into all forms of digital media in a way that is imperceptible to humans yet persists with the file through format changes and nonlinear distribution paths with little or no impact on the file’s integrity or fidelity. Reading devices equipped with special software detect the payload to facilitate lookup of the file and appropriate responses by a wide range of applications.

## CONTENT PROTECTION

Beginning in the late 1990s, digital watermarking was considered a viable solution to the problem of content piracy. Ever since digital distribution became mainstream, the content industry has struggled to control its distribution channel by employing a combination of strict licensing to authorized distribution partners, legal enforcement to impose limits on copying and redistribution of copyrighted content, and digital rights management (DRM)—a collection of technical measures designed to protect content from unauthorized use.

During the past decade, DRM became a cornerstone of investment by major companies involved in digital content distribution. Digital watermark-

ing, although a different technology originating in the broader discipline of steganography, was subsumed into the category of DRM applications.

In this same time frame, the content, information technology (IT), and consumer electronics (CE) industries engaged in lengthy negotiations to create a comprehensive watermark-based standard for protected music.

The resulting Secure Digital Music Initiative (SDMI) was an ambitious effort requiring the cooperation of all constituents in the value chain. It called for a new SDMI-compliant format, a standardized player, and a system that enabled copy control through the use of both robust and fragile watermarks. The robust watermark was designed to persist through digital file transformations, while the absence of the fragile watermark identified unauthorized copies.

SDMI was a relatively complex solution that required expensive implementation overhead on the part of CE manufacturers. Moreover, it was developed during the age of Napster’s free peer-to-peer (P2P) content sharing. Adoption of the new standard was also hurt by the concurrent, exponential rise of the MP3 format. SDMI consequently failed in late 2001, and industry members were left somewhat jaded about their

ability to achieve consensus on a mainstream watermarking solution.

## WATERMARKING AND DRM

Despite SDMI’s failure, watermarking found success in the prerelease markets for music, theatrical, and TV content. Unlike SDMI, proprietary watermarking solutions worked well in these markets as there was no need to impose the solutions on parties that had no interest in adopting them. They also reduced the significant financial losses of prerelease piracy and internal leaks early in the production and marketing cycles.

In addition, leading watermarking technology providers developed solutions for other emerging applications, such as using watermarks in digital cinema implementations to help law enforcement determine which specific theater a camcorder copy came from. Watermarking-based approaches for monitoring both airplay and ad verification on radio and TV broadcasts also took hold, as did widely deployed audience measurement technologies for broadcast content from industry leaders such as Nielsen.

In the face of the unrelenting onslaught of P2P distribution, several major content companies have begun championing mainstream watermarking solutions as a substitute for DRM, while others have thrown up

their hands, advocating completely open, “naked” DRM-free distribution, as recently offered on Apple’s iTunes and Amazon.com. A major music label’s recent experiments to include watermarking in MP3 distribution indicate that the technology continues to find favor among digital content distributors.

### BUSINESS DRIVERS

Unlike DRM, which is based on the premise that only explicitly licensed uses of content are allowed, watermarking doesn’t necessarily impose a priori restrictions on the use or interoperability of content. This in itself is a huge business advantage because it doesn’t negatively impact consumer enjoyment.

However, watermarking could also be used in some media, such as Blu-

ray discs, to achieve the same goals as DRM. It’s important to note that in such applications, watermarking typically supplements the underlying encryption-based technology. For example, Blu-ray disks use watermarking to augment the Advanced Access Content System (AAC) encryption-based DRM scheme, which is used to protect the content.

### Watermarking doesn’t necessarily impose a priori restrictions on the use or interoperability of content.

Currently, the content industry is interested in adopting digital watermarking technology in new applications to

- demonstrably deter piracy and reduce the resulting financial losses, especially early in the release cycle;
- increase sales by exploiting new and innovative business models for value-added digital distribution of content;
- provide reliable and automated reporting of content use at the right level of granularity so that

- revenues from both linear and nonlinear distribution can be fairly and appropriately allocated to all parties involved in the distribution chain; and
- increase consumer engagement through improved content search and targeted ad pairing based on content and opt-in.

These motivations represent a remarkable change in content owners’ attitude—from a strict command-and-control emphasis on explicitly allowed content usage to enabling substantially more on-demand enjoyment of content. This change is the first step toward the creation of watermarking-based applications that can help balance content owner business requirements with consumer choice.

### APPLICATION AREAS

Watermarking applications for digital content distribution fall primarily into one of three major categories:

- *Flag-based applications* use the watermark as a flag to enable copyright communication and enforcement. The watermark must survive normal transformations but isn’t subject to DRM interoperability restrictions. Examples include SDMI and Blu-ray.
- *Forensic applications* use the watermark to detect where or how a piece of content left the authorized domain. Examples include prerelease watermarks, digital cinema, transactional watermarking, and media serialization for music and video on demand.
- *Content-identification-based applications* use the watermark to enable innovative business models for content distribution

while enhancing the consumer’s ability to experience the content. Examples include filtering, management, measurement, and tracking.

Each application has different requirements for the following attributes:

- payload-carrying capacity;
- robustness, or the ability to survive transformations and attacks;
- imperceptibility, or the ability to minimally impact the fidelity of the content experience;
- level of security; and
- computational power to embed and detect the watermarks depending on the scale and latency requirements.

Leading technology companies and service providers are regularly delivering solutions in the first two application categories, proving that digital watermarking can either augment a DRM system or in some cases be a viable substitute in online audio, video, and image applications. The Digital Watermarking Alliance ([www.digitalwatermarkingalliance.org](http://www.digitalwatermarkingalliance.org)) provides a comprehensive list of these providers with case studies of successful deployments.

The third category includes some of the most promising future watermarking applications. Some content-ID-based applications extend traditional DRM technologies or serve as a substitute for encryption-based content protection. Others use content identification to solve problems related to tracking content flows rather than strictly controlling content usage. (B. Rosenblatt, “Content Identification Technologies: Business Benefits for Content Owners,” white paper, 15 Apr. 2008, GiantSteps Media Technology Services; [www.giantstepsmts.com/whitepapers.htm](http://www.giantstepsmts.com/whitepapers.htm)).

Content-ID-based applications need the right infrastructure to be

successful. They require the formation, deployment, and nurturing of an infrastructure by supportive partners including content owners, service operators, device manufacturers, advertisers, applications, and various technology and middleware providers.

However, unlike the experience of SDMI, these applications don't need all-encompassing standards that must be embraced by every constituent in the digital distribution value chain. All that is required is for at least one set of participants to have the right incentives to adopt these innovative new services.

## BUSINESS MODEL INNOVATION

A core premise behind the deployment of content-ID-based applications is the need to monetize distribution such that revenue is shared equitably while ensuring a fair price for the consumer. This requires rethinking the overall business model while engaging various participants early, keeping an eye toward rapid innovation and experimentation.

In addition to working through various legal and technical issues, content providers must form a compact with consumers and devise a new set of administrative and policy decisions. For example, using digital watermarks to identify content in an ad-supported model instead of in a download-to-own model would necessitate changes in distribution agreements and contractual compliance up and down the value chain.

Video and some music websites are currently testing ad-supported models. Service providers could also create "carrot-based" promotional scenarios and unique offers for legitimate users by combining a content ID payload with other information such as a retailer ID, a distribution method ID, and even media-serialized unique content.

For example, a digital retailer ID on the user's player application would

make it possible to offer retailer-specific bonus content or promotions to the consumer. Validation/authentication could occur by activating a lightweight watermark detector on the client side when the consumer downloads the watermarked content from the retailer's site, or by detecting a small portion of the original watermarked content on the retailer's server.

Further, promotional content can be customized using a distribution method ID. For example, consumers who have previously purchased download-to-own music tracks for 99 cents could get completely different offers than those who pay upwards of \$100 per year for a subscription. Heavy users of ad-supported music could also get "frequent-flyer miles" to accumulate prize tiers, access to artists' raw studio cuts, and so on.

A band, movie studio, or music label could likewise make special offers using the content ID itself to identify the music track, movie, or label. Promotional premiums could include concert ticket discounts, special screenings, "meet the director" or "meet the artist" events, "roadie for a day" contests, and so on.

Once content owners agree on the payload schema and other watermarking technology criteria, they must establish mandates for the licensing and distribution process. In a nonlinear ad-supported scenario that encourages viral distribution and syndication, the watermark acts as an embedded "bar code" to persistently identify the content itself as well as the copyright owner. Watermark detectors deployed at various choke points in the distribution network report on and monetize content flows per the established business rules.

In an age of heterogeneous devices requiring portability and interoperability of content formats, it's up to providers to define digital watermarking use cases in both DRM and non-DRM scenarios based on business models or application needs. For example, age-rating information

can be embedded within the content itself, enabling devices to impose usage rules designated by parents who register the device as belonging to a minor.

While developing innovative business models, it's important to consider privacy issues during the design of target applications. Watermarking itself doesn't impose any privacy risks. However, like other technologies, it could create problems if implemented in ways that fail to consider prudent privacy principles in the design and the handling of data generated by the target application. To address this potential concern, in May 2008, the Center for Democracy and Technology issued a white paper, "Privacy Principles for Digital Watermarking" ([www.cdt.org/copyright/20080529watermarking.pdf](http://www.cdt.org/copyright/20080529watermarking.pdf)), enumerating a well-defined set of best practices.

**A**lthough much work remains to be done to create viable business models, the technical underpinnings to implement robust, scalable, and efficient content distribution systems involving digital watermarking are already available. Leading vendors have been perfecting the state of the art with security considerations in mind for the past several years. With participants' commitment to fairly share in the risks and rewards of the requisite investments, watermarking promises to be a powerful tool to unleash unprecedented growth in the content industries as consumers enjoy media when, where, and how they want it. ■

*Rajan Samtani is director of business development at Digimarc Corp., a watermarking technology company based in Beaverton, Oregon. Contact him at [rajan.samtani@digimarc.com](mailto:rajan.samtani@digimarc.com).*

**Editor: Simon S.Y. Shim, Dept. of Computer Engineering, San Jose State Univ., San Jose, CA; [simon.shim@sjsu.edu](mailto:simon.shim@sjsu.edu)**