

**Digimarc Comments to USPTO regarding Technological
Protection Systems for Digitized Copyrighted Works**
***Technology, Education, and Copyright Harmonization
(TEACH) Act of 2002***

January 14, 2003

DIGIMARC

Digimarc Corporation
19801 72nd Ave., Suite 100
Tualatin, OR 97062 USA

© Copyright 2003 Digimarc Corporation. All rights reserved.

Table of Contents

Digimarc Comments to USPTO regarding Technological Protection Systems for Digitized Copyrighted Works	1
1 Executive Summary	3
2 Rights Management	3
3 Illustrative Examples	4
4 Answers to USPTO Questions.....	5
5 Background.....	7
6 Digital Watermarking Overview.....	7
7 Protection of Digitized Copyrighted Works	10
8 Digital Watermarking Applications for Protecting Copyrights	11
9 Conclusion	13
Appendix.....	14
1 Digimarc Overview.....	14

1 Executive Summary

One of the most promising technologies to help protect digitized copyrighted content, in conjunction with legal remedies, is digital watermarking. Digital watermarks are digital data embedded within the content, where the digital data can be read by machines but is not noticeable by people viewing or listening to the content. Digital watermarks provide a critical and economically feasible content identification and security layer that enables copyright holders to protect and track distribution and use of their content.

Complementary digital rights management (DRM) technologies, such as encryption and digital flags, provide good protection for content in digital formats but are rendered completely ineffective when the copyrighted content is converted into analog form.

Nearly all copyrighted subject matter is rendered in analog formats, such as in television, radio, books and magazines. The analog rendering is essential whenever the subject matter is consumed by humans because our “receivers,” our eyes and ears, are and will always be analog. Digital watermarks provide a crucial segue between the digital and analog domains, in that the digital watermarks are woven into the fabric of the content and survive digital/analog transformations, thus “plugging” what is known as the “analog hole.” Digital watermark technology can provide persistent identification of copyrighted subject matter to facilitate rights management in the emerging complex hybrid digital/analog devices and home networks. For both analog and digital content, digital watermarks enable copyright holders to protect their content from unauthorized use, as well as enable content owners to effectively communicate their copyrights, monitor use of their content, and track unauthorized distribution of licensed content. Digital watermarks can be used to support legitimate consumer expectations and other allowable uses, such as those permitted by the TEACH Act. Digital watermark solutions for images, audio and video are widely available from a number of companies and widely used - as billions of watermarked objects and millions of detectors deployed around the world illustrate.

2 Rights Management

Rights management is an increasingly important topic in consumer electronics, personal computing, and entertainment industries. Napster, the free music-swapping service, was the leading edge of a sea change in the management of copyrights. The entertainment and information technology industries are struggling to adapt and create new business models to accommodate this new world order. There are enormous implications for these industries and their consumers in the development and deployment of new models for distribution and consumption and the technologies that enable them.

Why is rights management so important? Rights management information will need to be attached to virtually every element of content to enable proper usage and reliable economic models. Rights management hardware and software will need to be able to identify content in a wide variety of analog and digital formats in many different channels of distribution across a varying array of devices to deter instantaneous and massive leakage of content into unauthorized channels. Failure to identify content in this

extremely complex situation will risk the collapse of the systems of economic rewards that foster innovation and creativity.

Entertainment represents only one type of content that needs new rights management technologies. Governments, schools and businesses are increasingly at risk to unauthorized super-distribution of their proprietary information, including copyrighted subject matter and confidential information. Rights management may soon be a standard part of the security infrastructure of all institutions, much like locked files, password-protected PCs, firewalls and virus protection.

Efforts to deal with these new challenges are in their infancy. Experts estimate that less than 1% of Internet content - whether business or entertainment related - has any rights attached to it. Digital watermarking can identify the content and link to the rights. As such, it is a promising technology that can form an integral part of the foundation of the new generation of rights management made necessary by advances in digital media processing and the global proliferation of the Internet.

3 Illustrative Examples

Digital watermarking is already used in a variety of copyright protection applications. Overviews of three examples that demonstrate the ability of digital watermarks to help protect, manage and enhance copyrighted content – in both analog and digital formats – are presented below.

3.1 Protection and Enhancement of Images on the Web

Digimarc ImageBridge™, introduced in 1996, is a broadly adopted solution that provides protection and enhancement of digital images. ImageBridge™ enables a content owner to persistently identify the image as copyrighted with a digital watermark. ImageBridge™ detectors exist in most image editing software, such as Adobe Photoshop™, and can be downloaded free of charge for use with Microsoft Windows® and Internet Explorer. Millions of copies have been distributed that detect the digital watermark and identify to the user that the image is copyrighted. ImageBridge™ further enables a consumer, such as a graphic designer, to link from the image that they are interested in via their PC to a web site chosen by the owner of the image. This web site can enable licensing of the image, provide a high resolution version, or promote related images, thus enhancing the value of the image, facilitating licensing, and enhancing ease of use for the consumer. The inherent copyright notice provided by the digital watermark also reduces inadvertent copyright infringement, where the consumer mistakenly assumes that the image is not copyrighted. There is a companion web spider service, MarcSpider™, which searches for digital watermarked images on the Internet, and reports back to owners of images where their images are used. This enables an owner to track image usage for proper billing or enforcement actions, thus protecting the image copyrights.

Similar solutions for monitoring use of copyrighted content and reporting its use to copyright holders is also available for broadcast audio and video such as radio and TV broadcasts, as identified in Section 7.3.

3.2 Forensic Tracking of Illegitimate Audio

It is common practice for music labels to provide CDs to music critics and radio stations as promotions prior to commercial release. Pre-release music has been increasingly showing up on the Internet, disrupting the orderly commercial introduction of the music. Audio digital watermarking is being used by the recording industry to identify pre-released CDs with the intended the recipients (with appropriate labeling) via a forensic watermark. Digital watermarking provides a covert digital identification of the music that can be used to trace the source of the unauthorized distribution.

3.3 Copy Protection of Video

DVDs are protected with the Content Scrambling System (CSS). Despite CSS, it is quite easy for consumers to make unlimited copies of the copyrighted video from the analog signal outputs of DVD players and digital copies can be made on a PC through use of circumvention programs such as DeCSS. These pirated copies, now stripped of any rights protection technology, can be further shared “in the clear” using physical media and the Internet. In response to a request for proposals from an alliance of leading companies in the motion picture, computer and consumer electronics industries, the Video Watermarking (VWM) Group, a consortium of companies that includes Digimarc, Hitachi, Macrovision, NEC, Philips, Pioneer, and Sony, has developed a digital video watermark that prevents the illegitimate copying of movies to DVD recorders, and enables copy once functionality, if desired.

4 Answers to USPTO Questions

In the United States Patent and Trademark Office’s (USPTO’s) request for written comments, the public was asked to provide answers to the following three questions:

(1) What technological protection systems have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems?

Digital watermark technologies provided by Digimarc and other companies are shown in Table 1¹.

¹ The applications are defined below in sections 6.6 and the trademarks are property of the respective companies.

Solution	Application
Images	
Digimarc Excalibur™	Forensic Tracking and Copyright Communications
Digimarc ImageBridge™	Forensic Tracking, Internet Monitoring and Copyright Communication
Signum SureSign™	Forensic Tracking and Copyright Communication
Audio	
Philips Audio Watermarking	Broadcast Monitoring, Forensic Tracking and Copyright Communication
Activated Content Audio Watermarking	Forensic Tracking
Verance Audio Watermarking	Copy Protection and Broadcast Monitoring
Video	
VWM (Digimarc, Hitachi, Macrovision, NEC, Philips, Pioneer, Sony)	Copy Protection
Philips WaterCast™	Forensic Tracking, Broadcast Monitoring and Copyright Communication
Philips Robust Video	Copy Protection, Forensic Tracking and Copyright Communication

Table 1: Digital watermark solutions by Digimarc and other companies

These solutions are based upon a secret key and open algorithm. The secret key can be renewed. The algorithm can run as a software process, even as part of hardware such as done with Philips WaterCast™, so that it is upgradeable.

(2) What systems have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process?

The Secure Digital Music Initiative (SDMI) adopted digital watermark technology from Verance for use in protecting music. This technology has also been deployed to protect DVD-Audio. A variant of the same technology has been deployed for monitoring of television and radio broadcasts.

A number of organizations are discussing use of digital watermarks as part of protection systems including: DVD-CCA's Copy Protection Technical Working Group (CPTWG); European Broadcast Union's Watermarking (EBU WTM) initiative; and Digital Video Broadcasting's Copy Protection Technologies (DVB-CPT).

(3) Consistent with the types of information requested by Congress, please provide any additional comments on technological protection systems to protect digitized copyrighted works and prevent infringement.

The rest of this paper responds to this question.

5 Background

This background section includes two important aspects of protecting digitized works: security assumptions and a description of a complete protection system.

5.1 Security Assumptions

To address the opportunities and challenges of protecting digitized copyrighted works, a widespread theory embraced by many copyright holders is that the goal should be to enable legitimate consumers to enjoy digital content while keeping honest people honest². To this end, this document defines the following security assumptions:

1. Protection should be easy to use for the legitimate user
2. Protection should support uses enabled by law
3. Protection should not be jeopardized by a consumer using legitimate tools or software³
4. Protection should enable the adoption of innovative content usage models and new digital equipment providing benefits to consumers

5.2 Complete Protection System

Security is obtained by designing a complete protection system based upon these assumptions, the threats, and the constraints. The constraints include balances between costs of implementation, costs of breaking the system, losses based upon the breaks, legitimate consumers' expectations to content portability and use of their legacy equipment, ease of use, and uses enabled by law. The protection system should consist of a combination of security layers, and must be analyzed in terms of the complete system, not the individual security layers.

6 Digital Watermarking Overview

Digital watermarking systems embed data in digital and analog content to persistently label the content with imperceptible identification or instructions, with which the content can be protected, managed and enhanced. Digital watermarks are generally imperceptible to the human eye and ear, but can be readily detected by DVD recorders, digital cameras, computers and other devices enabled by appropriate software.

6.1 Digital Watermarks work with all Media Types

Digital watermarks can be embedded in all media types, including images, documents, audio, and video. The digital watermark will survive printing for images and documents, and playing for audio and video.

² Professional piracy is based upon earning revenue and can be discovered and stopped via legal measures based upon the large amount of content the professional piracy ring must distribute.

³ This does not include piracy tools with no legitimate usage, which can be stopped via the Digital Millennium Copyright Act (DMCA)

6.2 Digital Watermarks are Effective

Digital watermarks are robust to normal processing and conversion to analog and back to digital, even several times. In other words, most standard consumer equipment will not accidentally remove the digital watermark. For example, the digital and analog outputs of devices rendering protected content will contain the digital watermark to signal the protection policy. The digital watermark will survive the standard processing of the content through the device, including resizing or brightening for rendering, such as printing or displaying on a TV. For the analog outputs, digital watermarks are critical since encryption and flags will have been removed.

Just as with all encryption technologies, which have suffered historically from widespread attacks and breaches of the protection system, it may be possible for a highly-skilled researcher or hacker to maliciously remove a digital watermark. However, there is high value in the digital watermark providing a layer of security for the vast majority of content as it is used by consumers. In addition, watermark removal greatly degrades the quality of the content, whereas when encryption is broken the content is perfectly recovered and available for un-authorized distribution.

6.3 Digital Watermark Keys are Renewable and Upgradeable

Common digital watermarking algorithms use keys. The key is used to embed and detect the watermark. This key can be public, where the public has access to a detector that reads the digital watermark. This is desirable in applications, such as copyright communication (more in section 8), where a general public detector is optimal. This key can also be private, in that only one entity, such as one movie studio, has access to the key for the embedder and detector. This is desirable in applications, such as broadcast monitoring and forensic tracking (more in section 8), where the content owner does not want others to be able to detect their digital watermark.

This key can be updated to renew the system. The algorithm can run as a software process, even as part of hardware such as done with Philips WaterCast™, so that it is upgradeable.

6.4 Digital Watermarks Can Reduce the Cost of the System

A complete copyright protection system generally has several security layers, each of which has some impact on workflow and consumption. The cost of a digital watermark detector is minimal in relationship to implementing the complete protection system. Digital watermarking is generally one of the least expensive elements, in terms of process impact, since it becomes an integral part of the content itself.

For example, a broadcast flag solution may require components to be updated at the various uplink and downlink transmission points to ensure its survival (similarly as required with analog equipment for VBI-based ATVEF triggers). Whereas the digital watermark can be embedded at the broadcast head-end or anywhere else in the broadcast process, and will remain with the content for its lifetime without updating any legacy broadcast or receiving equipment.

6.5 Digital Watermarks are Broadly Adopted

Digital watermarking is a deployed technology with billions of watermarked objects and millions of detectors in the market, supporting various applications. Digital watermarks are used in a variety of counterfeit and piracy deterrence solutions. Digital watermarking is currently deployed as an effective security feature in both printed and digital content. Digimarc is under contract to a consortium of the world's leading central banks to deter PC-based counterfeiting of currency. Television and radio broadcasts are being monitored via digital watermarking to audit syndication royalties and advertising runs, and for market research. Digital watermarking also has been adopted by music labels to track unauthorized distribution of pre-release music and provide record control for DVD-Audio. In summary, digital watermark solutions are widely deployed and being used today to protect digital content and help identify and track copyright infringement.

6.6 Digital Watermarks support Legacy Equipment, Consumer Expectations, and Distance Education

Digital watermarks do not stop legacy equipment from accessing the content, thus supporting consumer's expectations of legacy digital equipment working with new digital content as they are accustomed to having it work with analog content. After legacy equipment has accessed, stored, and/or processed the content, the digital watermark can be read when this content is re-associated with a new digital device that knows how to read the digital watermark.

In addition to working with legacy equipment, digital watermarks can be part of a protection system architecture that enables copy once or moving content within a home, but blocking redistribution outside the home, thus supporting consumer's expectations to be able to backup digital content and move it around the home.

Finally, since digital watermarks identify content and enable policy to be enacted, they can be used to protect content while enabling the uses supported by law, such as for distance education in the TEACH Act. In fact, as described above, digital watermarks can protect content while enabling the distance educator to use legacy equipment. Digital watermarks can also protect digitization of analog works as covered by the TEACH Act.

6.7 Digital Watermarking and Encryption are Synergistic

Encryption is similar to locking content in a safe, thus preventing unauthorized access. On the other hand, digital watermarks are woven into the fabric of the content and provide persistent identification and instructions, from which associated policies can be enabled. These synergies are summarized in Table 2.

Feature	Encryption	Digital Watermarks
Digital and Analog Formats	Digital only - does not survive conversion to analog	Both - including several conversions back-and-forth
Rendering	Does not survive	Survives
Legacy Devices	Cannot render content	Can render content
Compliance	Only compliant devices can render content and support related applications	Compliant and legacy devices can render content, but only compliant devices enable applications
Applications	All described in Section 8	All described in Section 8
Analogies	Lock in safe	Woven into fabric

Table 2: Digital Watermarks and Encryption

7 Protection of Digitized Copyrighted Works

Encryption and flag based solutions can provide a security layer for digital content and communications, and watermarking can provide a security layer for both analog and digital content and communications. One of the greatest concerns for copyright holders is the recently publicized issue of how to protect content that is vulnerable to piracy through the “Analog Hole.”

7.1 The Analog Hole

The analog hole can be defined as follows. Content, when converted into analog format (with the ever-present possibility of conversion back into digital form), loses any encryption- or digital flag-based security. This includes all consumer end-use of the content as well as all analog distribution and storage of content. For example, documents are converted to analog when printed, audio is converted to analog when sent from the CD player to the stereo amplifier and speakers, and video is analog when sent to one of the 273 million analog TVs or played on a digital or analog TV. This analog content can be copied in either analog or digital formats and redistributed. Digitizing the content is as simple as scanning a document, recording an audio file with the sound card provided on every computer, or recording with a video capture/tuner card (probably soon to be provided on every computer). It can be done by an average consumer with no special equipment since the current security architecture provides the PC with an unprotected analog input. Then, this digital copy can be shared with millions of users of Internet based file sharing systems – sometimes inadvertently and without knowledge of how the user may be infringing copyrights.

More details on the analog hole can be found at www.digimarc.com/spotlight/analog.

7.1.1 Example: Broadcast Flag is not Sufficient due to Analog Hole

One protection proposal – the broadcast flag – is akin to a fence with the gate left open. The proposed flag technology does nothing to protect played content or, e.g., the analog connection between a digital set-top box (STB) and TV. Thus, this analog content easily can be digitally recorded and redistributed. This enables an average consumer, without any special equipment, to easily bypass the Broadcast Flag. As such, the Broadcast Flag

does not represent a technically sufficient solution, and, thus, does not represent an activity that is worth the significant implementation costs to industry and consumers that are involved.

However, a Broadcast Watermark could protect the analog output of digital receivers (i.e. STBs). It would also be backwards compatible and preserved with legacy DTVs and DVD players to continue to support consumer expectations of use of their existing equipment.

7.2 The Analog Hole is Huge and Forever

The analog hole will exist forever. This is immutably true because the ultimate consumers – human beings – will always consume the audio and video content with their analog ears and eyes.

For images and documents, most people still prefer to read a printed copy of a report as opposed to reading a document from a PC or e-book reader.

For video, there have been suggestions to mitigate the effect of the analog hole by banning analog outputs. Such an unrealistic quest would be devastatingly costly for consumers. The analog receiver market is huge. TVs and related products are often very large purchases within family budgets, and have a useful life of at least 10 years. A forced early sunset of these products would cost consumers hundreds of millions of dollars of lost utility. This would create an unnecessary hardship for consumers in the 105 million households with 273 million analog TV sets or the 92 million households with analog VCR's in the United States.

Similar experiences in the audio market reinforce the fact that analog connections will remain. Despite two decades of digital audio (CD), analog connections between the CD player and amplifier remain the principal form of communication.

7.3 Digital Watermarks: Analog and Digital Security Layer

Since digital watermarks survive content conversion between digital and analog and back again, they provide a security layer useful for all digital and analog content and communications, and offer a layer of protection that plugs the analog hole. There are many applications in which digital watermarking can protect copyrighted works.

8 Digital Watermarking Applications for Protecting Copyrights

The digital watermark payload contains either or both

- Local machine control data
- Persistent identifier

The local machine control data can control the actions of the detecting equipment without requiring a remote database. The persistent identifier links the content to a database, usually remote, which contains information about the content, content owner, distributor, recipient, rules for use, etc. From this payload structure, digital watermarking can be

used in many applications to help protect, manage and enhance content. Among the applications available to support the protection of copyrighted content are the following:

8.1 Copyright Communication

Digital watermarks enable content owners to communicate their copyrights, usually in a public system, thereby helping to protect their content from unauthorized use and promoting legitimate licensing of the content.

8.2 Copy Protection

Digital watermarks enable embedding of copy and play control instructions within the content. These copy control instructions might indicate that play out is allowed, that a single copy can be made, or that no copies may be made. Compliant devices, such as digital video recorders, use this embedded information to determine whether copying or playing is permitted.

8.3 Broadcast and Internet Monitoring

Digital watermarks enable content owners and distributors to track traditional broadcast and Internet dissemination of their content. Content is embedded with a unique identifier, and, optionally, distributor and time information (for audio and video). For traditional broadcasts, detectors are placed in major markets, where broadcasts are received and processed. For the Internet, spiders track the Internet, especially known unauthorized sites, and send content to detectors. The digital watermark is decoded and used to reference a database, resulting in reports to the owner or distributor that the content played in the given market or web site, at a given time, and whether it played to full-length (for audio and video).

8.4 Forensic Tracking

Digital watermarks enable content owners or service providers to track where content left the authorized distribution path. The digital watermark can identify the authorized recipient of the content. Thus, copyright infringement can be tracked to the authorized recipient and appropriate steps taken to ensure future infringement is prevented.

8.5 Rights Management

Digital watermarks identify the content, and link to appropriate usage rules and billing information in conjunction with a digital rights management (DRM) system. This makes it easier for the mass market to purchase legitimate content, rather than use illegitimate content for free. Digital watermarking enables digital rights management (DRM) systems to connect content outside the DRM back to the DRM. More specifically, digital watermarking allows content to pass through the analog domain and over legacy equipment while still carrying information to be reintegrated with the DRM system.

9 Conclusion

A complete system for protection of digital copyrighted works must protect the content in both the digital and analog domains, support reasonable consumers expectations of using content and legacy equipment, and not interfere with uses permitted by law, such as for distance education. The analog hole must be addressed in such a system.

Digital watermarks are an economically feasible and proven security layer in such a system. Digital watermarks are transparent to the legitimate user, enable consumer expectations of using content and for legacy equipment to function properly, and work synergistically with encryption. Digital watermarks identify the content and enable application of an appropriate usage/protection policy.

Digimarc and other companies have and are deploying a wide range of solutions to address these needs, resulting in the watermarking of billions of pieces of copyrighted works and the widespread deployment of detectors in consumer products used by millions of consumers around the world.

Appendix

1 Digimarc Overview

Digimarc Corp. (NASDAQ: DMRC), based in Tualatin, Ore., is the leading provider of digital watermarking components and technologies used in a wide range of security, identification and brand protection applications.

Digimarc ID Systems, LLC, based in Burlington, Mass., and a wholly owned subsidiary of Digimarc, is a leading global provider of secure and durable personal identification solutions. It is the leading producer of driver's licenses in the U.S. providing systems and services to 35 states. Internationally, Digimarc ID Systems produces identification documents for more than 65 governments around the world.

Digimarc has an extensive intellectual property portfolio, with 79 issued U.S. patents with more than 1,700 claims, and more than 300 pending applications for U.S. patents, in digital watermarking, personal identification and related technologies. Please go to www.digimarc.com for more company information.