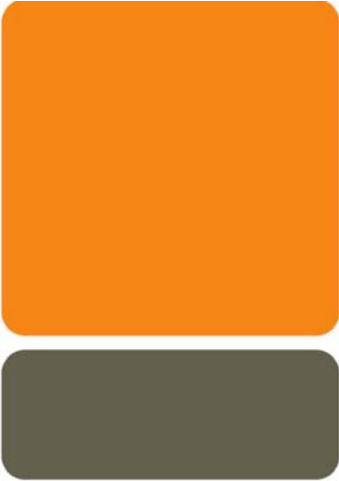


**WHITE PAPER****EXECUTIVE SUMMARY**

The music, movie and distribution industries are at a crossroad. On one hand, digital distribution of music and movie files offers new channels to market, and new revenue opportunities for the industry, while satisfying the desire of millions of consumers to digitally consume entertainment content. On the other, this same copyrighted content can easily be converted to compressed files, known as "ripping," and these compressed "ripped" files are easy to distribute in peer-to-peer (P2P) environments, online communities and other places where content can be uploaded and shared without systems in place to identify copyrighted content or to ensure the content owners receive proper payment or credit. Digital watermarks provide a solution to this problem, enabling content identification that gives the media and entertainment industry as well as individual content owners a means to enforce their rights while offering consumers access to legitimate content, when and where they want. Using digital watermarks, content owners can embed content identifiers and digital media serial numbers into music, movies or TV programming content that can communicate copyrights and usage rights. Since the digital watermark data inherently survives the ripping process and format conversions, copyrighted songs, movies, TV or radio programming and images can be identified on a P2P system and online communities such as MySpace, YouTube, Google and Yahoo, even after that content has been ripped.

P2P AND ONLINE ECOSYSTEM ISSUES

Music CDs and movie DVDs, along with online download services, provide what can be considered a digital master that users can turn into quality compressed audio or video files (a.k.a. ripping), such as MP3 files, and share those files on P2P systems or online communities without proper compensation to the content owners (e.g. record labels, musicians, song writers, filmmakers, etc.). Even with attempts at protection using encryption, CDs and digitally distributed songs or DVDs and movie clips can be recorded and digitized from the analog outputs (a.k.a. analog hole), or captured within the digital buffers of sound/video cards, and turned into unprotected audio and video files that are easy to share. Thus, P2P and online content sharing systems have difficulty determining which audio or video files are copyrighted and not allowed to be shared or require license rights and which files are non-copyrighted or allowed to be shared.



Successful commercial deployments of digital watermarking by the music, movie, broadcasting and advertising industries are already having a significant impact on reducing piracy in pre-release music and movies, and improving the ability to monitor, track and manage digital media. Digital watermarking enables the re-association of basic meta data (artist, song or movie, copyright) that has been lost during the ripping process. Digital watermarking opens the door to new and legitimate business models, new protection methods, and enhanced consumer experiences by providing additional related content in a “connected media” fashion that truly enhances the entertainment experience and links users to additional information or commerce opportunities.

OVERVIEW OF DIGITAL WATERMARKS

Digital watermarks can enable P2P systems and online communities to determine copyrighted from non-copyrighted content files within the existing distributed system architecture. Digital watermarks can even enhance P2P systems and online communities, enabling the P2P and online content-sharing providers to work with content owners to legitimately sell copyrighted songs and movies and related items.

As background, digital watermarks are digital data elements that are embedded into actual content—not carried in the header—so the elements survive analog conversion and standard processing, such as ripping to MP3. Digital watermarks may be embedded into, and read from, video, audio and still images for the applications described in this paper. For video content, watermarks in the audio, video or both the audio and video tracks may be used. The digital watermark data is not perceptible to the human ear (or eye), but can be read by computers. The digital data is secured through secret keys similar to encryption keys.

The digital data can include copyright control information, content classification flags for filtering, content identification (content ID) and digital media serial numbers, which can enable downstream forensic identification, for example. This data can enable numerous applications, including copyright communication, content filtering, copy protection, broadcast monitoring, Internet monitoring, forensic tracking, authentication, digital asset management, digital rights management (DRM), and enhanced e-commerce. Copyright communication, content filtering, DRM and enhanced e-commerce are most applicable to P2P systems and online communities.

Digital watermarks are in extensive use around the world, with billions of digitally watermarked objects and hundreds of millions of detectors in use for copy protection, copyright notification, authentication and forensic tracking applications. Digital watermark technology providers (and members of the Digital Watermarking Alliance) include Cinea, Digimarc, GCS Research, Jura, MediaGrid, Media Sciences International, Philips Electronics, Signum, Teletrax, Thomson, Verance, and Verimatrix. Major record labels and movie studios currently use digital watermarks to forensically track most pre-release CDs and DVDs. The system has led to a significant reduction in illegitimate use of pre-release music and movies, and has led to arrests by the FBI for pre-release Academy Award screener copies of movies.

In addition, a number of digital watermarking providers are helping major content owners in the media and entertainment industry today to mark currently distributed movies and music with unique identifiers.



Digital watermarking allows greater and safer dissemination of copyrighted works while at the same time ensuring appropriate compensation to the owners.

Digital watermarking has been deployed in conjunction with licensed DVD-audio implementations to prevent playback of unauthorized copies. Many theatrical releases and DVDs now carry audio watermarks inserted into this content by several major motion picture studios. This alone has created an ecosystem of tens of millions of pieces of marked content. Video watermarking solutions, which contain rights assertion information and have been proposed as the technology of choice for “Analog Hole” legislation, will create millions more marked digital media assets, if legislation passes.

Audio and video watermarks are being widely deployed by major broadcasters, music and movie studios and advertisers to help manage and monitor their distributed media.

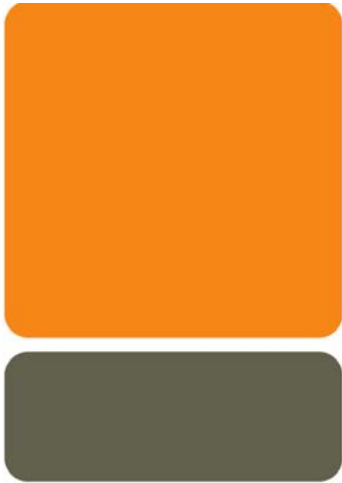
The above examples demonstrate that with hundreds of millions of currently distributed music, movies and TV programs carrying digital watermarks, P2P and online content-sharing providers could easily deploy systems to detect digitally watermarked content ingested into those systems and help ensure proper usage or compensation in accordance with rights.

ARCHITECTURE TO LEGITIMIZE AND ENHANCE P2P AND ONLINE SYSTEMS

Digital watermark systems have an embedder that adds the digital data into the content, and a detector that reads the digital data. In a P2P or online content sharing system, the architecture enables content owners (e.g., record labels or movie studios) to embed a secure copyright digital watermark (DWM) into digital content files, and allows software client applications used by the infrastructure providers to detect the digital watermark in content files when indexing those files that the user has allowed to be shared. The architecture details are described below and shown in Figure 1.

The content owners use a digital watermark embedder to embed the copyright DWM in the audio or video master, such that the DWM is included in all retail versions of the song or movie. The embedder is only available to legitimate producers of content, using standard distribution methods for security protection systems. The presence of a secure copyright DWM identifies the file as copyrighted work, and contains a content ID to identify the asset. For example, the copyright DWM acts as a flag to identify the presence of a copyrighted work, and the content ID is used to provide content specific information and services as detailed below. A copyright flag and content ID may be integrated into a single digital watermark or carried by separate digital watermark signals.

The digital watermark detector can be securely integrated with P2P or online community software that is ingested into a community site or downloaded by the user. The detector is used to look for a DWM on each audio or video file that the user has enabled the software to share when it indexes these assets to identify them for sharing. This indexing processing already occurs in P2P systems, and is usually run in the background and overnight. Adding DWM detection to the system will have negligible effects to the user (e.g., requiring a fraction of a second of additional processing per file on modern PCs or mobile devices), especially given that it fits with the existing distributed and run-in-the-background architecture for P2P or online community software.



The copyright DWM with the content ID can be used by the P2P or online provider to determine rights information, as well as other information about that file and related information, via a remote and potentially distributed database (i.e., to secure and enhance the content). This database can be stored where the provider stores the index database used to determine where to find files for search results. In fact, the database may comprise several databases where some parts of the database, such as song - lyrics, extra features, commentaries may be stored by the content owners, and can be used as additional revenue opportunities for all participants. These details can be determined by the P2P and online community provider and content owners.

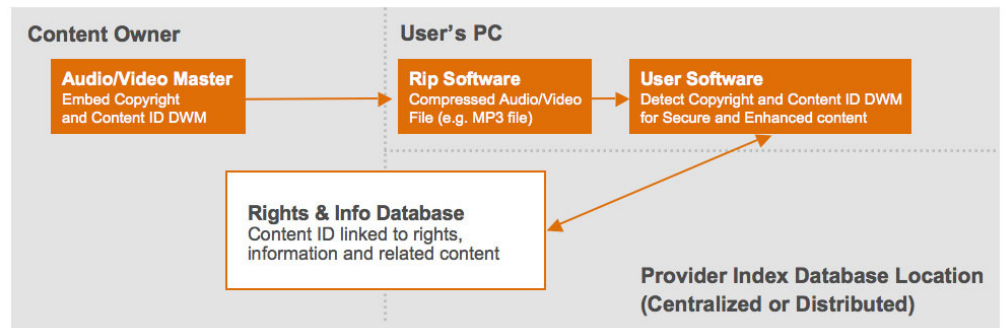


Figure 1: Overview of copyright digital watermark architecture

POTENTIAL USAGE MODELS AND BENEFITS

This architecture enables three usage models, including (1) copyright communication, (2) licensed content and (3) enhanced content, as describe below and shown in Figure 2.

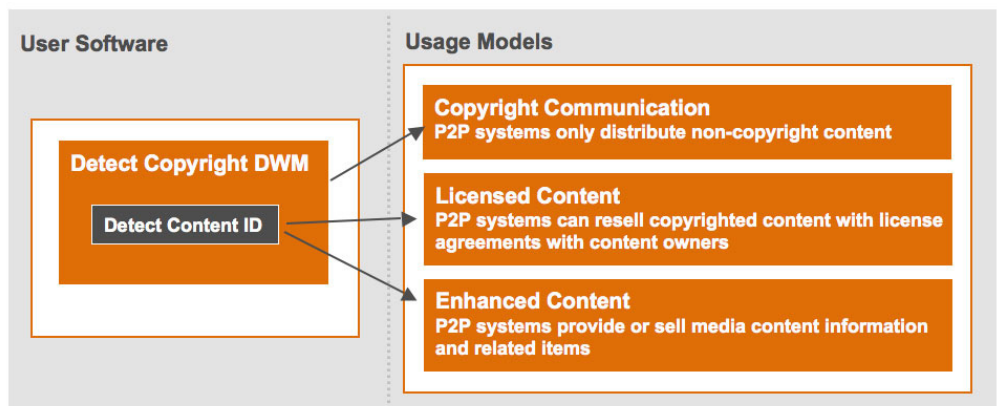


Figure 2: Overview of usage models



USAGE MODEL 1: COPYRIGHT COMMUNICATION

The copyright communication usage model would enable P2P and online community providers to prevent the listing of content where the copyright DWM has been detected during the indexing process. The copyright communication usage model does not require use of a content ID, thus being completely distributed and easiest to implement.

The benefits of this usage model are:

Consumers benefit by minimizing the risk of copyright infringement and potential legal liability by using P2P and online communities for legitimately licensed and non-copyrighted material

Content owners benefit by having less piracy and increased revenues from legitimately licensed content

P2P and online community providers benefit by minimizing risk of a lawsuit while enabling non-copyright and legitimately licensed distribution

Other manufacturers and service providers benefit because consumers have less fear of using computers on the Internet, which leads to more usage

USAGE MODEL 2: LICENSED CONTENT

The licensed content usage model would enable P2P and online community providers to detect the copyright DWM during the indexing process, look for a content ID, and use the content ID to look up the rights information about that content, and secure a copy of the content (or possibly a higher quality version) in a licensed form or a digital rights management (DRM) package, if allowed. The licensed or DRM package enables providers to sell the content to consumers after they have licensing agreements with the content owner.

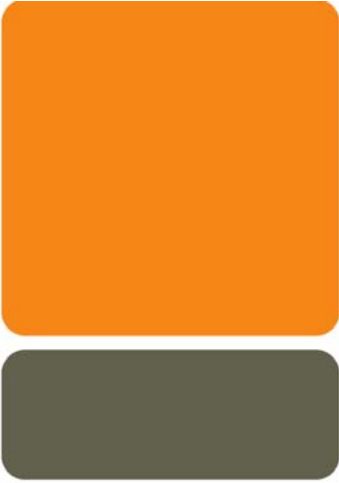
This usage model requires a slightly more complex architecture than for copyright communication, but also includes more benefits, including:

Consumers benefit by having more access to music and movies, leading to increased sales, as well as minimizing the risk of a lawsuit

Content owners benefit by selling more content and having even less piracy with improved content availability, as well as enabling non-copyrighted content distribution

P2P and online providers benefit by selling more music and movies and having customers enjoy more product capabilities, as well as minimize the risk of a lawsuit while enabling non-copyrighted and legitimate copyrighted content distribution

Other manufacturers and service providers benefit by further increasing usage of computers, mobile devices and the Internet, and increased digital music sales leads to more content being played on more portable players



Some P2P and online systems may exclusively use copyright communication watermarks, whereas other systems may use copyright communication for files with a copyright watermark but no content ID or no agreement with the content owner, and licensed songs with a content ID and agreement for distribution with the content owner.

USAGE MODEL 3: ENHANCED CONTENT

The enhanced content usage model would enable P2P and online community providers to detect the copyright DWM during the indexing process and use the content ID to link that user and others searching for that content to related content and information.

The enhanced content usage model can work synergistically with the licensed content usage model, thus only linking the users to more information for songs or movies that the P2P and online provider have the legal right to sell. When both securing and enhancing the content, only the extra step of linking the content ID to related content, meta data and information is required beyond the process to secure the content. This combination usage model enables even more benefits, including:

Consumers benefit by having more access to music and related information, leading to increased sales, as well as minimizing risk of a lawsuit and using the system for non-copyrighted material

Content owners benefit by selling more content and having even less piracy with the improved content and related information availability, as well as enabling non-copyrighted distribution


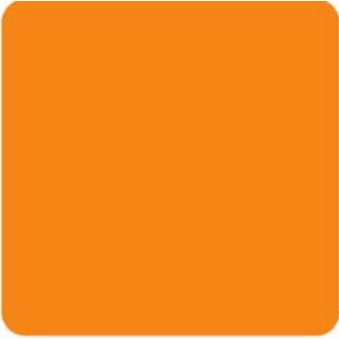
P2P and online community providers benefit by selling even more music, related items and having consumers enjoy even more product capabilities, as well as minimizing risk of a lawsuit and enabling non-copyrighted distribution

Other manufacturers and service providers benefit by increase usage of computers, mobile devices and the Internet and even more content to be played on more portable players

Once content is identifiable in any format through a digital watermark, e-commerce can be enhanced. The digital watermark is read and linked to more information about the artist or content and “buy now” opportunities. For example, a song played on a cell phone can be identified with a digital watermark, the content ID can be used to look up information about the artist, and other songs from that artist which can be purchased with the click of a “buy now” button. The possibilities are numerous; however, the process must start with efficiently identifying the content with a digital watermark.

DIGITAL WATERMARKING AND FINGERPRINTING ARE COMPLEMENTARY

Given the distributed architecture of the P2P or online system, digital watermarks are synergistic and complementary with audio and video fingerprinting (a.k.a., robust hashes) and are also more secure and efficient than using metadata, such as file name, or song title or copyright flag in the file header, to identify copyrighted content. Further, digital watermarks can explicitly identify unique instances of audio and video files and can also be used without requiring access to a central database, enabling more



flexible business models and allowing the digital watermark to link to information and services that are tailored to a particular distribution or usage context. The ability for digital watermarks to indicate specific versions of a piece of media and the channel from which it was originally distributed (e.g. VOD, optical disc, download-to-burn) allows for content owners to expand their ability to monetize this content as it proliferates P2P or online distribution channels. The ability for a watermark to create a digital “serial number” also allows for the ability to forensically track the source from which illegitimate content has been provided.

Meta data is easy to change, a copyright flag in file headers is simple to remove and fingerprinting can be altered through the addition of data or alteration of the audio or video. In contrast, digital watermarks have no or minimal database issues, and they are secured with a secret key, as used in encryption. This greatly raises the cost of piracy, thus reducing its likelihood, especially if legitimate content is easy to obtain.

In summary, digital watermarking provides a comprehensive, efficient and user friendly approach for identifying content that is complementary with other methods for identifying content as it is distributed.

CONCLUSIONS

Digital watermarks provide an easy-to-use and -implement approach to legitimize P2P and online community systems, and even enhance them. A copyright DWM is embedded by the content owner, and the copyright DWM is detected on ingestion into a community site or the user’s computer or mobile device to properly identify media files that the user has requested to be shared. This identification can lead to copyright communication, usage rights and licensing opportunities that legitimize online file-sharing systems, and even enhance them with sales of additional content and related items. This DWM architecture is synergistic with audio and video fingerprints and more efficient and secure than techniques using file names, song and movie titles or copyright flags, but can be used as a complementary layered approach with such systems.

Furthermore, the copyright digital watermark embedded by the content owners can be utilized for similar benefits in multiple distribution chains. It is even possible to use the same audio copyright DWM such that the P2P or online system searches for the same copyright DWM in all audio and video.

Digital watermarks can enable P2P systems and online communities to determine copyrighted from non-copyrighted files within the existing distributed ecosystem architecture. Digital watermarking can even enhance these systems, enabling the P2P and online providers to interoperate freely with existing value chain entities such as record labels and motion picture studios to market legitimate copyrighted content and other market related materials.