Journal of Intellectual Property Rights
Vol 9, July 2004, pp 313-331

Digital Rights Management: An Integrated Secure Digital Content Distribution Technology

P Ghatak, R C Tripathi, A K Chakravarti

Department of Information Technology, Electronics Niketan, 6, CGO Complex, New Delhi-110 003

Received 5 December 2003

The ability to distribute copyrighted works in digital form through high capacity prerecorded disks (CD ROMs, DVDs etc.) and Internet-enabled transmissions have brought new challenges to the protections of such content from unauthorized copying and use. Technological advancements in this regard are reviewed. Despite the ease with which digital content owners can now transfer data, images, music, video and multimedia documents across the Internet, current technology does not let them protect their rights to the works, which has resulted into widespread music and video piracy. In fact, although the Internet permits widespread dissemination of digital content, the easy-to-copy nature of digital data limits content owners' willingness to distribute their documents electronically. Digital Rights Management (DRM) technology is a key enabler for the distribution of digital content. DRM refers to protecting ownership/copyright of electronic content by restricting the extent of usage an authorized recipient is allowed in regard to that content. DRM technology has historically been viewed as the methodology for the protection of digital media copyrights. But DRM technology products can be leveraged to address much larger issues, including the control of rights and usage permissions of content and digital information. DRM presents the opportunity to package, price, distribute and sell content in many new ways that have never been possible before. The paper discusses about the digital medium, digital watermarking, copy protection techniques (CPT), important legal developments and issues, court cases, DRM applications, DRM technology overviews, and DRM enabling technologies and standardization. It also discusses about the initiative taken by the Department of Information Technology for a watermarking project.

Keywords: Digital medium, digital watermarking, copy protection techniques, information and communication technology

The rapid development of Information and Communication Technology (ICT) and ICT–based business in recent years, together with the advent of Internet has created electronic marketplaces with new technological, social, management and organizational issues. The progress of ICT has made it possible to convert all phenomena into digitized information, which can be shared and exchanged by the people all over the world by means of computer networks. This ability to distribute copyrighted content in digital form through Internet-enabled transmissions has brought new challenges to the protection of such content and information from

unauthorized use and copying. When CDs were first marketed in the mid-1980s, consumer digital recording of any kind was fair enough to be a commodity of the future and the implications of unprotected content were barely considered. No one had visualized the current pervasiveness of the Internet.

Despite the ease with which digital data owners can now transfer multimedia documents across the Internet, current technology does not let them protect their rights to the works. Today, there is no universally compatible, standard means of ensuring that the people who bring about the creative works – the artists, the musicians, the producers, the distributors, the broadcasters – get their fair share of user's money, every time a user obtains a piece of their work. There is not even an agreement as to how many times one should pay for 'content': once per viewing (listening), once per person, once per household, or once for everyone in the household.

Meanwhile, the technology needed to deliver that content – movies, audio tracks, TV shows, multimedia – is taking off to new heights. Obviously, the widespread dissemination of these technical advances that could boost both the consumer electronics and communications industry is being held back by the inherently different goals of the product and content creators. The consumer electronics industry wants abundant content to be readily and cheaply available to drive the sale of the new products needed to download, record, and play it. The entertainment people deservedly want remuneration for the use of their content – but what is the reasonable charge for different categories of contents to different class of users is a debatable matter. Thus, the need for a DRM system that protects intellectual property rights (IPR) in open network environments continues to grow. DRM systems are explicitly modeled on the copyright system which has always been a legal regime embedded in a technological system like the printing press and the analog and digital media[1].

The Digital Medium

Intellectual property is complementary to technology. It is an area of law that evolves with the development of technology to fulfill the social, political and economic needs. The emerging ICT, convergence of information technology and telecommunication along with the increasing use of computers and communication technology have given rise to digital economy. The new economy is changing the way the products are created, the nature of products themselves and how they are distributed and transacted. The ease with which authored works in digital form can be currently replicated poses a difficult problem for the law to handle[2]. In the existing copyright regime, making of copies for personal or private use without permission from the copyright holder is considered 'fair use' and lawful. Two factors limited the proliferation of analog copies – they had to be distributed on physical media, and the tape hiss and other noise introduced by the copying meant that none was even as good as the original. Copies of copies are close to

unbearable. Since in the digital domain, perfect multiple copies can be generated, it becomes even more difficult for the copyright owners to exercise control over replication of their works and seek compensation for unauthorized replication. On the other hand, the digital medium also provides a lot of scope for using restricting technologies like digital watermarking, encryption, password protection etc. against illegal copying of copyrighted material and commercial misuse of works.

Another characteristic of digital medium that poses problem for IPR system is the ease with which digital works can be transmitted and used by multiple users. A pirated version of a digital work (data, music, video, multimedia, software, etc.) can be loaded into a computer connected to a network of computers or Internet and transmitted to multiple users for simultaneous viewing and use of the same copy. Digital compression or compactness is another characteristic of digital media, which has potential to create new kinds of legal problems. In comparison to print and other traditional analog media, compressed digital works, like compressed zip files, MP3 music, MPEG videos, JPEG pictures etc. do not take much space and hence such works are inherently easier to steal. While the compactness of digital media makes it possible to put company records, whole libraries, encyclopedias, music, videos, photographs etc. in a set of CD-ROMs, DVDs, hard disks, some new kinds of IPR related law problems hitherto unheard of in the traditional print and analog world are likely to result from these new assemblies of materials. This has led to development of elaborate systems with access restrictions and regulations, which in turn, has thrown up issues of right to regulate, who should regulate, types of rights to be controlled and kinds of access to information sources[3].

Digital transmission of copyrighted works has enabled new services in the form of specialized news and data services, commercial online services, video-on-demand, web casting and TV music services. All these services function wholly or partially with Internet as the delivery medium. With regard to copyright, these services differ from the broadcasting and other delivery mechanisms of the past, as there may be no broadcaster involved. A wide variety of works and services are made available on a server of the service provider for interactive access and use at the time determined by the user. The amount of transmission traffic handled by telecommunication carriers for such interactive services has increased dramatically in recent years. Internet Service Providers (ISPs) provide a link between users and the telecommunication carrier, making the digital architecture more complex. When a user looks at the information on an Internet site, the copy being viewed is merely one that was made by the web site owners and transmitted to the user upon request from browser through HTTP and TCP/IP. In this case, copyright infringement issue becomes irrelevant because no one other than the copyright owner reproduced copies, prepared derivative works, distributed copies, as prescribed by the copyright laws. But for a user to be able to view the

work that was transmitted to the user's browser from the web site, a copy may have been created that resides at least temporarily in the RAM of the user's computer. Also multiple copies of the work may be made at the intermediate machines as it travels from source to destination. Effective copyright protection cannot be relegated to the point where content is on the transmission path of the Internet and the solution to copyrights in the digital medium must be independent of the internal architecture of the Internet. Digital medium is essentially technology driven and the IPR regulatory regime[3] must conform to the fast changing technology and hence must remain flexible, broad and technology – neutral to an extent possible.

Digital Watermarking

Digital watermarking is a technique that enables information to be embedded within digital content[4]. This information could be, for example, the copyright holder's identity or licence rules that apply to the content. Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in the protected form, the watermark remains in the content in its original form and does not prevent a user from listening to, viewing, examining, or manipulating the content. Also unlike the idea of steganography, where the method of hiding the message may be secret and the message itself is secret, in watermarking typically the watermark embedding process is known and the message (except for the use of a secret key) does not have to be secret. Watermarking is the direct embedding of additional information into the original content or host signal.

Ideally, there should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host signal.

Applications of digital watermarking include copyright protection, fingerprinting, authentication, copy control, tamper detection and data hiding applications such as broadcast monitoring. Watermarking algorithms have been proposed for still images, audio, video, graphics, text and multimedia. Requirements and design of watermarking techniques are impacted by the different types of content in two major ways: imperceptibility and

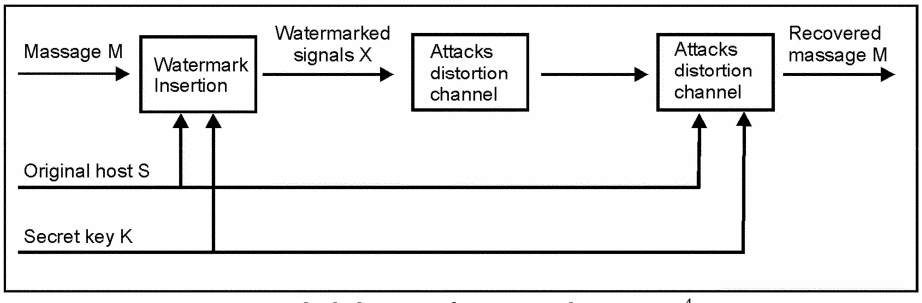

Fig. 1 — Block diagram of a watermarking system[4]

robustness. For the digital medium where thousands of content providers wishing to protect digital content after it has been delivered to consumers, the main application of watermarking is in embedding information within content to allow illegal copying and distribution to be detected. For this application, watermarks need to be 'robust' in that it should not be possible for consumers to remove the watermark without harming the quality of the content so much that it becomes worthless. This implies that the watermark must be embedded throughout the content; otherwise just the part containing the watermark could be removed. Some typical distortions or attacks that digital watermarking schemes are expected to survive include resampling, rescaling, compression, linear and non-linear filtering, additive noise, A/D and D/A conversion and transcoding. In applications of copyright protection, each copy gets a unique watermark to identify the end-user so that tracing is possible for cases of illegal use, and for authentication, where the watermark can represent a signature and copy control for digital recording devices[5]. Here the technical challenge is to provide transparency and robustness, which are conflicting requirements. Ideally, an effective, robust watermarking scheme provides a mark that can only be removed when the original content too is destroyed. Typically, many of the applications for copyright protection involve relatively high quality of original content and the imperceptibility criterion is critical for such applications. An important advantage of using robust, transparent watermarking for DRM is that the watermarks are transparent to consumers and to the software in existing content delivery systems so that they can be used with minimal impact on any existing system.

Recognizing that both analog and digital signals must be protected, copy protection technical group (formed in 1996 to explore techniques for protecting DVD content and composed of members of the MPAA, ITIC, CEA & RIAA as well as law firms and technology watchdog organizations) has for the last few years been exploring watermarking technology. But watermarking has proven to be a complex issue, and, despite many tests, the group has not yet decided on a single technique[6]. Two proposals are being evaluated by the watermark group, composed of Digimarc, Hitachi, Macrovision, NEC, Philips, Pioneer, Sony and Toshiba. These propose longer encryption keys up to a key length of 56 bits for protecting both recordable and pre-recorded media, and for making the key harder to break. New technology introduced by the group includes the media key block. This makes it possible to revoke compromised keys separately and without damage to the total encryption system. Another technique is actually an off-disc scheme, a transmission line protection system called digital transmission content protection. In finalizing the technology, group members have also to compare the cost of implementation with its effectiveness in blocking copying. Still, it is difficult to reach a consensus.

Copy Protection Techniques (CPT)

The CD audio format was invented by Sony Corp (Tokyo) and Royal Philips

Electronics, NV (Amsterdam, Netherlands) in the late 1970s as a replacement for vinyl records. Although it stores audio in digital form, CD audio format makes no provisions for data applications. In the early 1980s, compact disc read only memory (CD-ROM) was developed to specify discs that could be accessed from a computer and store data as well as audio. Recordable and rewritable CD formats (CD-R, CD-RW) were finally created in late 1980s and early 1990s after which the momentum on copying the discs began to build. One of the factors the companies focused on first for copy protection was the original standard that defined the CD audio format in 1980, known as Red Book. This has only one provision that allows for copy protection, the serial copy management system. This consists of a few copy-generation control bits slipped into the digital stream. Intended to prevent digital audiotape (DAT) recorders from making copies of copies, it has no effect on PCs.

The information stored on a compact disc is organized into functional units called *tracks*. A typical audio CD contains one audio track for each song, and a CD-ROM disc contains both audio and data tracks. Tracks are subdivided into blocks called *frames*, which hold 1/75 second of audio or around 2048 bytes of digital data along with error correction bits. Multiplexed with main data stream in each frame are eight subchannels. Only two subchannels, designated P and Q, are commonly used. The P subchannel marks the current track number, the track type (audio or data), and the time signature of the frame relative to the start of the disc. This data is displayed by the players and allows seeking a specific time position. There are two special regions: the *lead-in* area before the first track and the *lead-out* area after the last one. These consist of several empty frames that contain no audio but may include subchannel data describing the rest of the disc. The Q subchannel in the lead-in area holds a table of contents (TOC) specifying the number of tracks, their starting positions, and whether each contains audio or data. This is the basic CD format understood by CD audio players and CD-ROM drives. The CD-R and CD-RW writable disc formats have more complicated structures. CD-R media cannot be erased, so the standards were designed to allow data to be written incrementally until the whole disc is filled.

In the absence of any consensus on copy protection technology, several record labels and third parties have independently developed a family of copy-prevention techniques for CDs and DVDs. In general, these work by introducing intentional errors into the audio data or other structures on compact discs when they are manufactured. The errors are carefully designed to ensure that the discs work correctly in almost all CD players but are unusable in most PCs. All the protection systems used today exploit several key differences between audio players and the CD-ROM drives of computers. The goal is to prevent the unrestricted reading of audio data to PC. Audio players, for instance, interpolate over data-read errors, such as those caused by scratches, making it possible for copy protection schemes to introduce correct-

able errors that shouldn't be audible, but confuse CD-ROM drives. Such drives do not interpolate over errors; their primary use, storing computer files and applications, requires essentially perfect recovery of recorded data. When reading audio discs, they extract the data, byte by byte, even if it is an error. If lots of errors accrue, the result is badly flawed, unlistenable music file — exactly what the record labels want if a CD is copied. Adding deliberate errors to the CD master would seem to be a perfect solution since it can be done within Red Book framework. But if enough errors are introduced to ruin CD-ROM-drive ripping, the interpolation may become audible on CD players. In fact, if a CD bears enough bad data, the player may mute, skip, or even stop. So a balance must be struck between playability and protection.

A copy protection device now commonly being used is the Cactus Data Shield, produced by Midbar Tech (Tel Aviv, Israel, now a subsidiary of Macrovision Corp, Santa Clara, California, USA). To obstruct ripping from too many errors, Cactus alters the CD's table of contents (TOC), which points the player to the individual tracks, in ways especially difficult for CD-ROM drives to resolve. Cactus also adds a data "session", an extra track that only CD-ROM drives will find. When one tries to play the CD on a computer's drive, the alterations to the TOC make software players like Windows Media Player unable to locate the first audio track, causing the PC to load a proprietary player contained in the data session. That player will play the audio at a greatly reduced bit rate, and will not let anyone copy it.

Other copy protection schemes, like Macrovision's SafeAudio, alter the Reed-Solomon error-correcting codes normally used to ensure accurate data recovery. The alterations cause most CD-ROM drives to reject the related pieces of data. Playability is again at issue because CD players vary widely in their ability to accept apparently bad data. Some will play a flawed CD just fine, some will mute during extended interpolation attempts, and some will give up and quit. Adding errors may also shorten life of a CD because it reduces the capacity of players to interpolate over errors from accumulated dirt and scratches. With Macrovision's recent acquisition of Midbar Tech, SafeAudio is being supplanted by Cactus Data Shield. While Cactus also introduces some errors, it flags them as control data, making them a little less likely to damage because control data can more easily be ignored when playing a CD than can audio bits.

Sony Corp, which co-established Red Book, also offers Key2Audio copy protection system. While promising no changes to the audio bit stream, and thus no audio degradation, Key2Audio relies on a separate data session and some fiddling with the disc's TOC to confuse PCs. But early versions of Cactus and Key2Audio have been thwarted by users who obscured the data session, which is near the edge of the disc, simply by scribbling over it with a felt-tip pen. To prevent further manipulation, both Midbar and Sony have new versions of their products that make the line between the

data and audio sessions visually indistinguishable, so that the data session cannot be easily marked. A new entrant into the fray is Microsoft Corp (Redmond, Washington, USA) with its new second session technology. This adds an extra data session containing Windows Media Player files and a set of rules for their use.

Still, given the open nature of Red Book's digital audio, and the widespread file swapping on the Internet, it's unlikely that today's music can be protected. It takes only one person with a digital CD player-to-PC connection to rip songs and spread them around. And, of course, all these protection methods address only digital data streams. A good analog transfer, easily made by connecting a CD player's audio outputs to a computer sound card's audio inputs, sounds indistinguishable from the original. It creates a swappable file that neatly bypasses all the schemes.

New standards, like DVD-audio and super-audio CD, offer superior sound quality and leave behind the Red Book format, contain robust copy protection and support copyright management system[7]. Super Audio Compact Disc (SACD), developed by Sony & Philips, is viewed as the successor of the standard CD. Most SACDs consist of a high-density (HD) layer (4.38 GB Capacity), glued on top of a standard CD layer. Besides high-quality stereo, high quality multi-channel audio is also offered on the HD layer of the disc. Both versions are stored in Direct Stream Digital (DSD) instead of pulse code modulation (PCM). Not only does SACD provide an enhanced listening performance to the end-user, it also provides strong copy protection for the music industry. To combat the problem of music piracy, SACD used a set of complementary means of visible and invisible security to ensure that the content of SACD is very well protected. SACD does not rely in any means on audio watermarking. The most apparent anti piracy measure is the inability of existing PC disc drives to read data from an SACD disc. This is enabled by scrambling of the lead-in data area using a technique called "SACD Mark". Assuming one would succeed in reading the SACD data, the data cannot be used, not even after a bit-identical copy has been made. When an SACD disc is inserted in a player, the player searches for an invisible (physical watermark). This pit signal processing physical disc mark (PSP-PDM) is required to start playback and to descramble the audio content. Since existing consumer recorders cannot write a PSP-PDM, the next barrier would be to remove the PSP-PDM scrambling. However, removing the PSP-PDM would require breaking an 80-bit code, which is different for every SACD. The code is never visible on a bus or connecting between integrated circuits (ICs), not even in scrambled form. The descrambling in a player is done in dedicated ICs by licensed IC manufacturers. PSP-PDM encoders are not available on the open market and can only be leased from Philips intellectual property and standards. Since unlicensed DVD mastering equipment cannot write PSP-PDM, pirated discs will miss PSP-PDM.

DVD-audio specification was drawn up in cooperation with the music indus-

try, which demanded very high quality audio in stereo and multichannel, multimedia functions and security. Digital Versatile Disk (DVD) offers more than six times the storage capacity, four times the frequency range and 256 times the resolution of CD. For the high quality audio, DVD-audio adopts a new copy protection system: content protection for pre-recorded media (CPPM). Additionally, audio data on a DVD-audio disc may contain an 'audio watermark' that enables downstream control of illegal copying. CPPM technology together with copyright management information on the disc protects the recorded content and aims to control any copying. CPPM uses encryption to protect content in the AUDIO_TS directory. An audio track can optionally include an audio watermark. The watermark can carry copy control information (WM-CCI) and other information about the copyright holder, which may be used to trace illegal copies. Under the CPPM contract, audio data must do the CPPM-encryption when a WM-CCI is included that restricts copying. Therefore, a non-CPPM disc, which contains such a watermark, will be an illegal disc. Players supporting CPPM detect the watermark and stop playing back such discs.

Like CDs, DVDs, which were first introduced in late 1990s, also potentially allow unlimited copying with no degradation from one generation to the next. Here the encryption system adopted to prevent copying was the content scrambling system (CSS). With CSS in place, home copying of DVDs was curtailed, but in October 1999, a software utility called DeCSS was created by a Norwegian programmer, Jon Johanssen, which broke the CSS scrambling and allowed the reading of encrypted DVDs. The DeCSS code was posted on the Internet and the CSS, the linchpin behind DVD security, could be unlocked virtually by anyone. To curtail DVD copying, Royal Philips Electronics, NV, is promoting 'disc wobble' (also called wobble groove) technology[6] as a solution. This technique encodes hidden protection data onto the lead-in groove along the inner edge of a DVD in a difficult-to-duplicate manner. Normally, a DVD's grooves form a smooth spiral, with the data encoded as reflective and absorptive spots along the path. Disc wobble reshapes the groove by wiggling the path back and forth ever so slightly in a pattern that conveys the ons and offs of digital data. Used in conjunction with watermarking, disc wobble could ensure that watermarked content would be played only from wobbled– that is, authentic– DVDs. Because of sophisticated tools needed to manufacture such discs, pirating wobbled discs would be next to impossible, at least for now. In fact, today's DVD players will become obsolete if and when these new measures are encoded on all DVDs.

Important Legal Developments and Issues

In December 1996, the World Intellectual Property Organization (WIPO) concluded work on two treaties (WCT & WPPT) designed to bring copyright protections into the digital age. A core concept in these agreements is the prohibition against circumvention of technical measures employed to protect copyrighted

content from unauthorized copying[8]. Technological protection measures require appropriate legislative and legal support to ensure that these measures are respected and to deter the defeat of such measures by parties that might otherwise, violate the rights of content owners. While the WIPO Treaties (WCT & WPPT) set forth the general prohibition against circumvention of technological measures, each signatory of the WIPO Treaties must implement the WIPO Treaties through the enactment of national laws such as the Digital Millennium Copyright Act (DMCA) of 1998 enacted by the United States and the Directive on aspects of copyright and related rights in an information society, enacted by the European Union. With requisite quota of countries already signing WCT and WPPT, it has now become obligatory for countries like India to suitably enact the provisions of these WIPO Treaties in their existing national laws. The Administrative Ministry for Copyrights, Ministry of HRD is currently in the process of bringing Amendments to the Copyright Act, 1957, to include suitably the necessary provisions of these two Treaties[9].

The DMCA prohibits circumvention of technological measures that effectively control access to copyrighted works and prohibits devices that circumvent technological measures that effectively protect a right of a copyright holder[10]. The bill includes exceptions from the circumvention prohibition for libraries browsing works to determine whether to purchase them, law enforcement and intelligence activities, reverse engineering for the purpose of achieving interoperability with other products, encryption research, protection of privacy and security testing. Copyright Management Information (CMI) of a digital work consists of the title and other information identifying the copyrighted work; the name of the author; name of the copyright owner; with the exception of public performances by radio and television broadcasting stations, the name of the writer, performer or director; terms and conditions for use of the copyrighted work; identifying numbers or symbols referring to such information or linking to such information; such other information as the Registrar of Copyrights may prescribe by regulation. The DMCA prohibits knowingly providing or distributing false CMI, the international removal or alteration of CMI without the consent of the copyright owner, and distribution of the copyrighted works with removed or altered CMI. Watermarks are considered CMI because they convey the owner's identity and the terms and conditions for use of copyrighted works. Consequently, the removal of watermarks without the consent of the copyright owner amounts to infringement under DMCA.

The EU Directive on aspects of copyright and related rights in the information society specifies that Member States shall provide authors, performers, phonogram producers, producers of the first fixation of films, and broadcast organizations, the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, of their copyrighted works[11]. Two narrow exceptions are allowed for transient or incidental temporary reproductions if such reproductions are made to

enable (a) a transmission in a network between third parties by an intermediary or (b) a lawful use of work where there is no economic benefit associated with the reproduction. The Directive specifies that Member States shall provide authors, performers, phonogram producers, the producers of first fixations of films, and broadcast organizations with the exclusive right to authorize or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them. This aspect of the Directive prohibits entities from making copyrighted works available over the Internet unless authorized by the copyright holder. Regarding protection of technical measures and rights management information, the Directive specifies that Member States shall provide adequate legal protection against the circumvention of any effective technological measures. The Directive also requires Member States to provide adequate legal protection against any person knowingly removing or altering any electronic rights – management information, e.g. watermarks. In the absence of voluntary measures taken by the rights holders, the Directive specifies that the Member States shall incorporate 'appropriate measures' in their national law to allow circumvention of technological measures by (1) libraries, educational establishments, museums, and archives for non-commercial ends; (2) broadcast organization making ephemeral recordings; (3) teaching and scientific research organizations; (4) to individuals with disabilities; and (5) for purposes of public security. The Directive further specifies that Member States may incorporate appropriate measures in their national law to allow circumvention of technological measures by natural persons seeking to make a reproduction for non-commercial ends, unless each reproduction has already been made possible by right holders. These exceptions to the anti-circumvention requirement are much broader than the narrow exceptions provided in the DMCA.

Both the DMCA and EU Directive were designed, in part, to encourage efforts by content owners and makers of computers, consumer electronics and telecommunications devices to develop and license DRM systems to protect content and to establish standards for such systems. While the US Congress passed the DMCA in 1998, the European Union (EU) is apparently moving in the slow lane when it comes to establishing rules to protect copyright holders in the digital age. The EU's copyright directive has not yet been approved by the European Parliament (Strasbourg, France), let alone be adopted by its member states. The deadline for the adoption of the directive passed at the end of December 2002 with just two countries, Greece and Denmark, signing up.

Court Cases

Two high-profile cases[6] have tested the limits of this anti-circumvention law. The first, *Universal City Studios Inc* v *Corley,* involved DeCSS, the computer program that decrypts the CSS encryption used to

prevent DVD copying. When DeCSS became available on the Internet, film copyright owners sued the operators of web sites that posted DeCSS software or linked to sites that did. The trial court in New York City in 2000 ruled DeCSS a prohibited circumvention technology that did not come within any of the law's narrow exceptions – a ruling upheld on appeal. The court also ruled that disseminating DeCSS – including by offering links to web sites where the program was available – was illegal even though users might circumvent the encryption and use the film on the DVD in a way that copyright law allowed.

Another case raises issues of technological protection measures beyond the territory of familiar copyrighted material such as motion pictures or e-books. *Lexmark International Inc* v *Static Control Components Inc* involves a computer chip that laser printer maker Lexmark placed in its printers. That chip apparently prevents the printers from using toner cartridges other than those made by Lexmark. The suit alleges that Static Control makes computer chips that circumvent this technological protection measure, allowing the printer owner to use non-Lexmark toner cartridges. In February, a federal judge in Kentucky ordered Static Control to stop making or selling its chips, pending further consideration of the case.

By far the highest-profile digital copyright case to date has been the suit against Napster on file sharing[8], which disseminated software that let users participate in a peer-to-peer (P2P) network in which they could transmit digital music files to one another. Although the files were transmitted directly from user to user, the software had to connect to Napster's central server to locate other users and the files available on their computers. The major record labels and others sued the company, claiming users were infringing copyright and Napster was legally liable for those infringements. A federal appeals court in San Francisco ruled in 2001 that many Napster users were likely infringing copyright in using the network. The court ruled, that Napster was doing more than supplying copying equipment (software), it was also operating a computer network. The company could be liable if it operated the network with actual knowledge that copyright infringement was occurring yet failed to block access to infringing transmissions. The court therefore ordered Napster to cooperate with copyright owners to filter infringing activity. Before the case could proceed to trial, Napster reached a settlement with some plaintiffs. Difficulty in complying with the court's injunction, however, led Napster to shut down its network in July 2001.

These cases, though not exhaustive, and the others that will surely follow, will define what legal and technological control copyright owners will have over how consumers use copyrighted works and how technology companies design and sell software and electronic devices.

Digital Rights Management (DRM) Applications

DRM is a technology that lets rights holders safely distribute and sell their content online in a digital form[12]. With

DRM content owners can configure access and usage rules for their own content. Access rules may address the price of the content, the frequency and duration of access, and whether the user is authorized to save, print or transfer the content to other users. This allows for new business models such as trial before purchase, promotional previews, rentals based on play counts or expiration dates, subscriptions, and purchases of streaming or downloadable media. For online content, owners can quickly change usage rules without having to redistribute the content. Considering the applications, the most promising content for distribution with DRM are :

- Audio : music and the audio materials
- Video : movies, music videos
- Publishing : books, documents, news articles etc.
- Multimedia presentations
- Computer games and software.

With DRM, books, market research, professional journals, etc. can all be securely published and distributed on the Internet. The publishers can gain access to new consumers, lower the costs of distribution, and greatly increase their knowledge of consumers' interests and needs. In addition, a provider can permit the re-use of all or portions of its information by others in the value chain, increasing collateral sales. Software can be securely downloaded or physically distributed to users, demonstrated, purchased or rented with payments and usage information going back to the participants (including the publisher, distributor and retailer) as determined by their agreements. The use of DRM software application during creation phase of digital content works towards creating a trusted environment where both the sender and the consumer can be assured that the content they receive was indeed sent by the appropriate party and the consumer is authorized to receive the content.

DRM Technology Overviews

DRM consists broadly of two elements : the identification of intellectual property (copyright) and enforcement of access and usage restrictions[12]. The identification consists in the attribution of a standard identifier and marking the content with a watermark. The enforcement works via encryption that is by ensuring that the digital content is only used for purposes agreed by the right holder. The first step in providing a deployable and expandable DRM technology strategy involves the appropriate metatagging of the contents that are created and stored within databases and digital media asset management technologies. After the assets are metatagged, the information is encrypted to ensure the security of the content. After sufficient authorization and clearing (e.g. payment) of the content , asset is accounted for, the content can be transmitted (a decrypted key unblocks protected content) and displayed in a secure and trusted environment via a client technology, like the Acrobat Reader, an Internet Browser, Media Player or a set-top box.

A DRM system usually has four software components[13]: content protection software, a content distribution server, a licence server and a content viewer plug in. Usually the DRM system is integrated with an e-commerce system that takes care of payments and triggers the functions of the licence server (Fig 2).

The DRM process starts with the content provider encoding and metatagging the content into the format supported by the DRM software. The format depends on the software vendor e.g. software from Microsoft only supports Window Media files. Next the content is encrypted and packaged using special access and usage

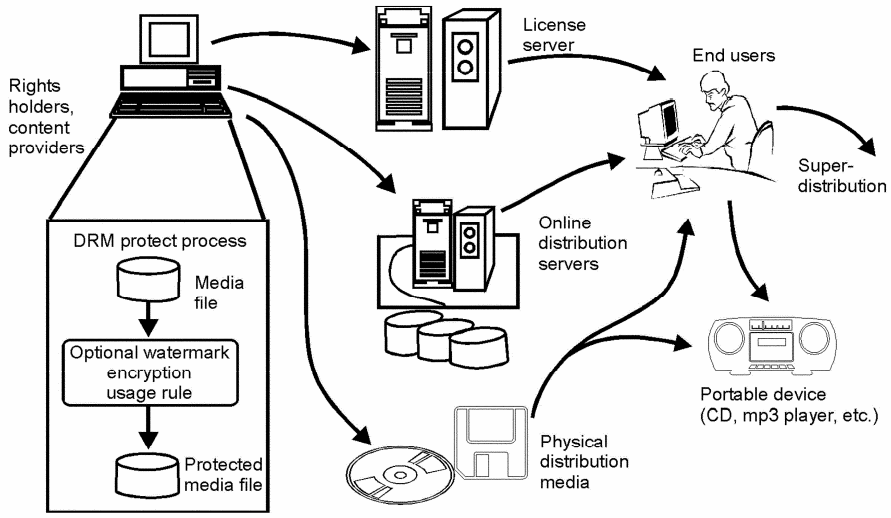

Fig. 2 — DRM process flow

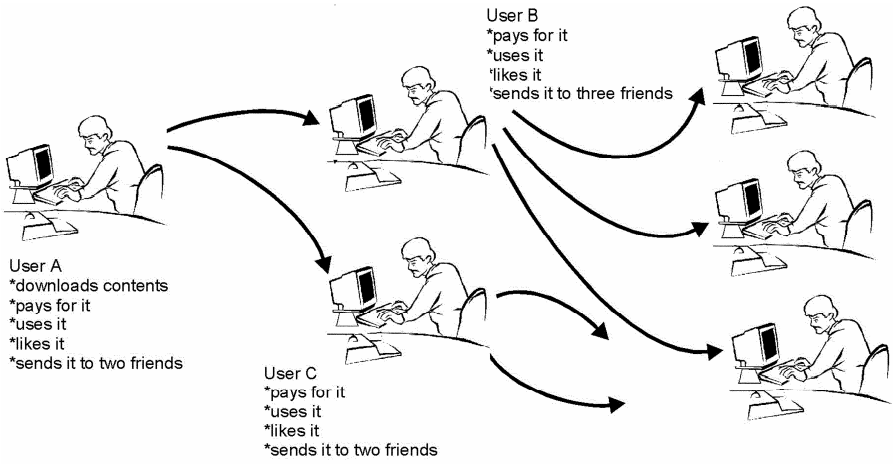

Fig. 3 — Superdistribution

rules or a licence key that is saved on the licence server or on the physical distribution medium such as CD or a DVD. The licence server consists of three components: (1) an encryption key repository, (2) a user identity database which ties back to the content, and (3) a DRM licence generator that binds the content and the encryption key to the end user's device and registers the user with the appropriate parties involved in the digital distribution value chain. Superdistribution is a special usage rule that accelerates the distribution of content and lowers the marketing costs substantially (Fig 3). The protected content is transferred to the appropriate distribution server or saved on physical distribution media. In the case of audio and video, the online distribution can be done using downloading or streaming. At the other end of the process is an online customer who downloads the protected content or wants to receive the content stream. The client software on the end user's device communicates the appropriate rights and permissions to the end user and back to the licence server. The number of communications back to the licence server is determined by the content rules at the time of packaging. Once the user abides by the appropriate registration (e.g. name, address, email), payment and clearing methodologies for operation, the DRM licence handler collects the user and content asset information and produces a licence to decrypt the content on the end user's device.

DRM is attracting a lot of interest at the present time, and there are a large number of companies and organizations working on developing such systems. Major companies include Microsoft, IBM, Real Networks, Sony and Inter Trust, to name just a few, which are working on both the component technologies of the system as well as providing completely integrated secure content delivery systems. Organizations include the Motion Pictures Association of America (MPAA), Secure Digital Music Initiative (SDMI) and Moving Picture Experts Group (MPEG). Microsoft's end to end digital rights management platform for secure distribution of digital media files is called Windows Media Rights Manager (WMRM) and currently supports only Microsoft's proprietary WMA audio and WMV video formats. IBM's product for DRM is called the Electronic Media Management System (EMMS). It has an open architecture that allows for future advances and changes in the various media properties, such as encryption, compression, and watermarking. The Real System Media Commerce Suite (RMCS) from Real Network is a platform for secure licensing and delivery of digital media. It includes typical DRM software components: content protection software, a licence server, an enhanced distribution server and an upgraded Real Player. Sony's latest 'Open MGX' DRM and distribution technology can be utilized for various types of products and devices. With this technology, the usage conditions for content can be controlled from the distributor's end and hence, content distribution can be secured from the beginning to the end of the service. Inter Trust Rights System, general purpose DRM platform enables the content owner to first encrypt pieces of content using the

standard packager or stream packager. Next, the usage rules are set and stored in secure files called rights packs. The encrypted content is stored on the retailer's distribution server and the rights packs are stored on the rights server. The rights client family consist of five products: rights desktop for PCs, rights TV for set-top boxes, rights phone for mobile phones, rights PD for portable music player and PDAs and rights PDF plug-in. Inter Trust's DRM solution cannot be used for streaming, which is a disadvantage considering the distribution of music and videos. In January 2003, Sony Pictures Entertainment and Phillips Electronics purchased the assets of Inter Trust Technologies. Inter Trust assets include 26 patents and 85 pending patent application for software and hardware, which can be implemented in DRM products.

DRM Enabling Technologies and Standardization

DRM system should enable rights holders to enjoy maximum flexibility, within legal boundaries, in setting the usage rule they wish to apply to their content, as well as enable them to adopt new business models, which open up new and alternative revenue streams for their content. For this, the deployment of a global and interoperable technical infrastructure, which would facilitate access for consumers and for all producers, should be encouraged. The need for any standard that is basically an agreement between interested parties comes from an essential requirement: interoperability. The key to effective standardization is to create a 'minimum' standard that normatively defines a minimum set of tools that will guarantee interoperability[14]. In the context of DRM, technologies where standardization is and will be essential are: content representation (including scalability capabilities), content and usage environment description, transport protocols and intellectual property management and protection of the associated descriptions and adaptations. Interoper-ability in DRM systems is very crucial to the realization of open multimedia infrastructure. Some of the open standards[14,15] that are being adopted for DRM include:

DOI (Digital Object Identifier)

DOI is a system for identifying and exchanging intellectual property in the digital environment. The DOI provides unique IDs for any content type. DOI is a system for persistent identifier of intellectual property entities on digital networks. It is a key standard in DRM since it is interoperable with almost any DRM technology. The DOI has two components, the prefix and the suffix, which together form the DOI. A DOI may be assigned to any item of intellectual property, which must be precisely defined by means of structural metadata. The DOI itself remains persistent through ownership changes, and unaltered once assigned. Unlike a URL, it does not point to a location.

XMCL (eXtensible Media Commerce Language)

XCML is an XML – based language for describing rights models, such as rights, attributes, types of users, security levels etc. XMCL aims to establish interoperability between proprietary DRM

systems by standardizing the rules for how content can be played in a way that is independent of codes, DRM system and e-commerce system.

XrML (eXtensible Rights Markup Language)

XrML is a language to specify rights. XrML is an XML-based usage grammar for specifying rights and conditions to control access to secure digital content and services. It is intended to support the commerce of digital content, such as the publishing and setting of e-books, movies, music and games and computer software. XrML provides syntactic, semantic and system interoperability. This interoperability enables XrML to be used as a part of a bigger system and comprehends other things such as security. Some of the companies supporting XrML include Adobe, HP, Xerox and Microsoft.

XACML (Extensible Access Control Markup Language)

XACML is an XML specification for expressing policies for information access over the Internet. Ratified by the Organization for the Advancement of Structured Information Standards (OASIS) in February 2003, XACML was developed to standardize access control through XML so that, for example, a user can access several affiliated website with a simple logon. The objective of XACML is to address the need for a common interface standard among diverse systems and devices by defining a language capable of expressing policy statements for a wide variety of information systems and devices. The approach taken by XAMCL is to draw together long-established techniques for access-control and then to extend a platform – independent language (XML) with suitable syntax and semantics for expressing those techniques in the form of policy statements.

OeBF (Open eBook Forum)

The Open eBook Forum (OeBF) is an international trade and standards organization whose members consist of hardware and software companies, publishers, authors, user of electronic books, and related organizations. The goal of the OeBF's standards activities is to produce industry-adopted specifications, which benefit publishers, technology companies and consumers. OeBF provides a forum for the discussion of issues and technologies related to electronic books and for developing, publishing and maintaining common specifications relating to electronic books and promoting the successful adoption of these specifications.

ODRL (Open Digital Rights Language)

ODRL provides the semantics for a DRM expression language and data dictionary pertaining to all forums of digital content. The ODRL specifications support an extensible language and vocabulary (data dictionary) for the expression of terms and conditions over any content including permissions, constraints, requirements, conditions, and offers and agreements with rights holders. ODRL supports MPEG-21 and has been officially accepted by the open mobile alliance – formally known as the WAP Forum – as the standards rights expression language for all mobile content. ODRL is freely available and has no licensing requirements.

OMA (Open Mobile Alliance)

OMA is an organization which seeks to develop the entire mobile industry by removing the barriers as global user adoption and by ensuring seamless application interoperability which allowing businesses to compete through innovation and differentiation. OMA has tackled the issues of downloading and distribution of digital content through mobile phones with the standardization work of the OMA download, which includes (i) applying DRM to content and its distribution, and (ii) enabling controlled (i.e. reliable) delivery of generic content objects. The OMA DRM Version 1.0 standard governs the use of mobile – centric content types, whether it is received by WAP download or MMS. This is the world's first mobile DRM standard. OMA has chosen the XML based ODRL as the basis of their digital rights expression language for content.

MPEG (Moving Picture Experts Group)

MPEG is an ISO/IEC working group for standards development of coded representation of digital audio and video. MPEG has a series of specifications promoting content interoperability pertinent to DRM: MPEG – 2 A/V content for DVD and TV, MPEG-4 multimedia content representation (Metadata), MPEG-4 IPMP (Intellectual Property Management and Protection) addresses connected appliances and standalone devices, MPEG-7 is content description (complements MPEG-4), MPEG-21 is a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by different communities. MPEG Rights Expression Language (MPEG REL) specifies the expression language for issuing rights for users to act on digital items, their components, fragments and containers. MPEG Rights Data Dictionary (MPEG RDD) forms the basis of all expressions of rights as defined by MPEG REL. The MPEG-21 REL & RDD work together to allow the machine-readable expression of rights associated with the use of multimedia.

SDMI(Secure Digital Music Initiative)*:*

SDMI is a forum of worldwide record industry, consumer electronics and information technology to develop specifications for music related DRM solutions. SDMI published a specification Part I, Version 1.0 for 1999 but its later Part II watermark proposals were successfully cracked. After this, SDMI has gone slow on its Phase II proposals and is presently unclear how important SDMI will be in future.

Department of Information Technology Initiative

The Department of Information Technology, Government of India, has initiated a project titled 'Watermarking of digital audio and setting up of resource centre for DRM systems' at Centre for Development of Advanced Computing (CDAC), Thiruvananthapuram. To start with, this resource centre shall develop robust watermarking algorithms for digital audio (PCM, MP3 etc.) and test and simulate those watermarking techniques as a copyright protection mechanism of digital audio over Internet. The project

also involves adoption of various international standards to develop DRM system for efficient and secured delivery of content (audio, video) over Internet.

Conclusion

There have been tremendous advancements in DRM and digital media management technology recently. Although traditional DRM has been viewed primarily as an anti-piracy technology, DRM provides for bigger revenue generating opportunities, especially in context computing, new business models, and new digital products. It is based on extracting the technological, legal, and economic functions of copyright to identify principles that should be the basis for the design of DRM systems. DRM is rapidly becoming an integral part of successful companies' corporate and Internet infrastructure. Besides different spending behaviour that might generate revenues for many online entertainment companies, the seamless management of rights ends its billing processes secure to improve today's entertainment experience in the PC, television and other portable devices environment using the emerging DRM technology.

References

1 Jean Camp L, 'First principles of copyright for DRM design,' *IEEE Internet Computing*, May-June 2003

2 Piva A, Bartoline F, Barni M, Managing copyright in open networks, *IEEE Internet Computing*, May-June 2002

3 WIPO's Digital Agenda – *www.wipo2.wipo.int*

4 Poditchuk Christine I and Delp Edward J, Digital watermarking: Algorithms and applications, *IEEE Signal Processing Magazine*, July 2001

5 Commission of the European Communities, Commission staff working paper- Digital rights, background, systems, assessment, Brussels, 14.02.2002, Sec.(2002) 197

6 *IEEE Spectrum*, **40** (5) 2003

7 Sun Microsystems white paper, Digital rights management: Managing the digital distribution value chain

8 Turnbull Bruce H, Weil Gotshal & Manges LLP, Important legal developments regarding protection of copyrighted content against unauthorized copying, *IEEE Communications Magazine*, August 2001

9 *IPR Manual version 2.0, General Information on Copyrights Protections of Software and other Digital Works*, IPR Cell, Department of Information Technology, Government of India

10 US Copyright office summary, The Digital Millennium Copyright Act of 1998, December 1998

11 Commission of the European Communities, Commission staff working paper- Digital rights, background, systems, assessment, Brussels, 14.02.2002, Sec (2002) 197

12 Sonera Plaza Ltd, Medialab, Digital rights management white paper, 3 February, 2002

13 Sun Microsystems white paper, Digital rights management: managing the digital distribution value chain

14 *CEN/ISSS Digital Rights Management Draft Report*, Feb. 2003 for European Commission

15 National Institute of Standards and Technology, US Department of Commerce, Special Publication 500-241, *Information Technology: A Quick Reference List of Organizations and Standards for Digital Rights Management, October 2002*

16 International Organization for Standardization ISO/IEC JTC1/SC29/WG11, *Coding of Moving Pictures and Audio, Intellectual Property Management and Protection in MPEG Standards*, January 2001