Appendix N

Digital Rights Management

Introduction

In Chapter 10, there was a mention of Digital Rights Management (DRM, see Box 10.2). There is more on DRM in this appendix. The links provided here about DRM products/solutions are meant for information only and in no way authors mean to recommend these products. It is up to readers, as per their own wish, to explore more on these services/solutions/products in DRM space.

Software piracy is on the rise worldwide as well as in India (see Refs. #5–7, Additional Useful Web References, Further Reading). Today many works exist in digital media and, therefore, protection of digital assets becomes a huge concern for the creators of those assets. Books published in electronic (known as "E-Books") can be read on a personal computer or now on special devices such as "Kindle." For E-Books, DRM is useful because using DRM one can create restrictions to limit or prevent copying, printing and sharing of E-Books. Electronically published books are normally meant for limited circulation and in such a case DRM is useful. Software piracy is an Intellectual Property (IP) offense. In the context of cybercrimes, it is important to know about "Digital Rights Management" or digital watermarks and therefore this appendix.

What is Digital Rights Management (DRM)?

The term "Digital Rights Management," abbreviated as DRM, is collectively used for access control technologies. DRM is utilized by companies that manufacture hardware. DRM is also used by publishers and individuals who try to impose limitations on the usage of "digital content" and devices. DRM can also be used by holders of copyright (see Section 10.2.1, Chapter 10). The term DRM sometimes gets sarcastically mentioned as "Digital Restrictions Management." DRM, as a term, describes technologies used for inhibiting uses (legitimate or otherwise) of digital content that were not desired or foreseen by the content provider.

Although not many understand this nuance, DRM normally does not refer to other forms of "copy protection" which can be overcome without modifying the file or device, such as license key, product serial numbers or keyfiles (file on a computer which contains encryption or license keys). DRM can also refer to limitations related to particular instances of digital works or devices. DRM is being used by leading music companies. Interestingly, however, even when DRM is prevalent for Internet music, some online music stores do not use DRM and they discourage users from sharing music. Thus, DRM is a technology used to create certain circumstances under which some digital media files – such as audio and video – can be used and shared. The terms for DRM usage are usually created by the owner of the piece of digital media (e.g., a music recording company where a song is in digital form). DRM is programmed in the file so as to make it irremovable. The DRM rules are thereafter used to decide how the file behaves on other computers.

Why DRM?

DRM has tremendous relevance for media and contents creation industry, especially for India. DRM is a technology for copy protection – it is meant for restricting the illegal distribution of copyrighted music. Forms of control can include limitations on the use of certain music players such as to how many times a purchased music file can be burnt to CD or the number of computers it can be transferred to.

Piracy is rampant in other digital asset creations too. For example, it is said that world over, more than 60% of all music which is downloaded is illegal. Music and content development industry in India is flourishing and the country is one of the top countries in the world facing a threat, with the music industry losing between US$ 600 billion and US$ 650 billion a year due to piracy. DRM is often used to stop illegal activities such as sharing of MP3s on file-trading networks or to ensure that people pay for the songs/music they download from the Internet.

Technologies for DRM

Although DRM technologies have been in existence for quite some time (see Table N.1), DRM is, in some areas, a very infamous technology, because some people say that it deprives consumers of the right they have in the physical world. In fact, there is quite some controversy around DRM – see the link mentioned in Ref. #1, Additional Useful Web References, Further Reading. On the other hand, media owners who use DRM argue that it is essential to make sure that owners get paid for their property/works.

Table N.1 DRM technologies and their usage scenarios

Name of the Technolgy	***Usage Since Year***	***Used In***
Digital Rights Management for Personal Computers		
Windows Media DRM	1999 and onward	Online Video Distribution Networks
FairPlay	2003 and onward	The iTunes Store, iPod
Helix & Harmony	2003 and onward	Real Networks Services Enterprise, business
Orion/EasyLicenser	2003 and onward	Networking, financial, telecom and consumer applications, business, educational
Excel Software	2006 and onward	Government and consumer applications
Adobe Protected Streaming	2006 and onward	Flash Video/Audio Streaming
PlayReady	2007 and onward	Computers, mobile and portable devices
Digital Rights Management for Portable Devices		
Janus WMA DRM	2004 and onward	All PlaysForSure Devices
OMA DRM	2004 and onward	Implemented in over 550 phone models
VHS Macrovision	1984 and onward	Video through the end of the 20th Century
Content-scrambling system (CSS)	1996 and onward	Some DVD Disks
DVD Region Code	1996 and onward	Some DVD Disks
ARccOS Protection	Perhaps since 1997	Some DVD Disks
OpenMG	1999 and onward	ATRAC audio devices (e.g., MiniDisc players), Memory Stick based audio players, AnyMusic distribution service
BD+	2005 and onward	Blu-ray Discs
DRM Technologies No More in Use		
Extended Copy Protection	2005	Sony and BMG CDs

Digital Watermarks and DRM

Digital watermarking technique enjoyed enormous demand when people started rampantly sharing information on the Internet. When people share files online, one will not know if someone is using the file without the person’s permission. People would want to put a stop to commercial use of their documents in an illegal manner – so you might either consider information like images with a worst pixel quality, for example, or you decide not to publish anything worthwhile on the Web. However, none of these are good ways of overcoming the problem of unauthorized use. In such situation, you would look for a more effective way of protecting your information even when it is published on the Web. One such method is *digital watermarking*.

"Digital watermarking," as a method, involves burning information into a digital signal in a manner that makes it hard to remove it. "Digital watermark" as a term owes its origin to a process used way back in the year 1282 in the production of paper, having a watermark to make identification in a visible manner. For the purpose of digital watermarking, the signal may be video, audio or even pictures. When the signal is copied, the information also gets inside the copy. Inside one signal there can be multiple watermarks of different types at the same time. Figure N.1 shows examples of digital marks embedded inside images.

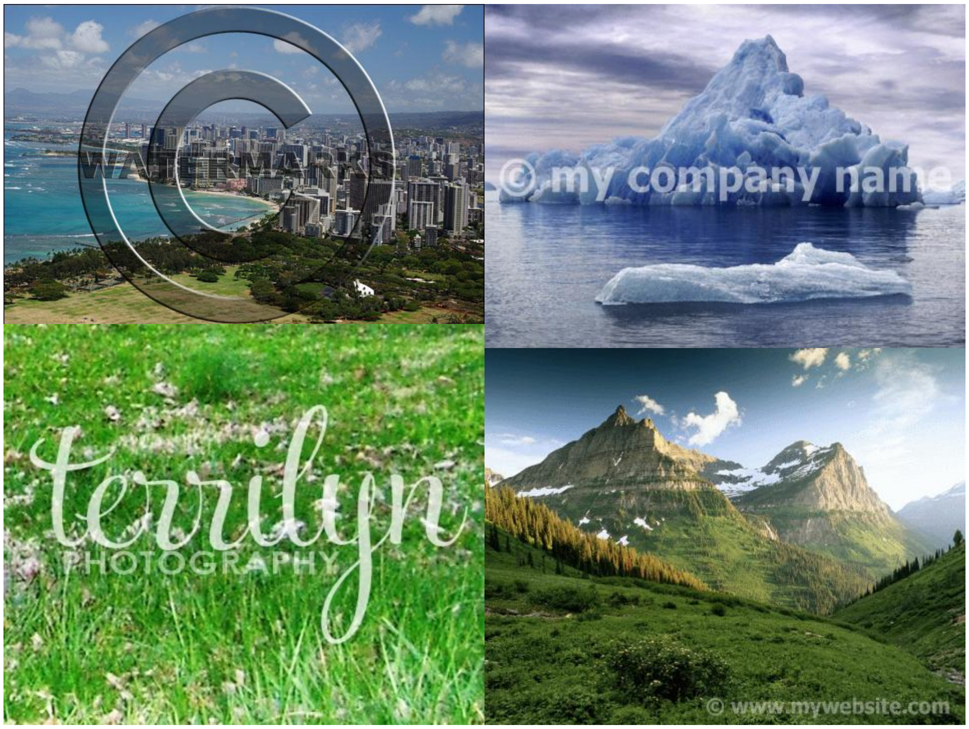

Figure N.1 Examples of digital watermarks.

Sources: http://en.wikipedia.org/wiki/Digital_watermarking;
http://www.google.co.in/images?hl=en&source=imghp&q=digital+watermark&gbv=2&aq=f&aqi=g2&aql=&oq=&gs_rfai=
Iceberg on right is from link:
http://bytescout.com/files/images/examples/watermarking/watermarked_image_sample_text_fits_page.png
(the Larger Image thru Google Image Search)
(29 December 2010).

Digital watermarks are classified on the basis of their "robustness," "perceptibility" and "capacity"; however, this discussion is beyond the scope of this appendix. To know more about digital watermarking classification, refer to Ref. #10, Additional Useful Web References, Further Reading.

A digital watermark is simply a bits-pattern that gets embedded into a digital file – image, audio or video. Such messages typically carry copyright information about the file. You may wonder how the term digital watermarking came into being – it actually came from the idea of "water marked" images that we see on the currency notes. However, there is one difference – digital watermarks need to be invisible or at least they should not change the perception of original file. This is, in contrast, to paper watermarks because these watermarks are supposed to be fairly visible. "Digital watermark" is the information that is to be embedded in a signal. However, in some situations the phrase "digital watermark" refers to the difference between the watermarked signal and the cover signal. The signal, inside which the watermark gets embedded, is the "host signal." A watermarking system is typically consists of following three distinct steps:

1. Embedding;
2. attack;
3. detection.

During the process of embedding, an algorithm accepts the host as well as the data to be embedded and the result is a watermarked signal (see Fig. N.2).

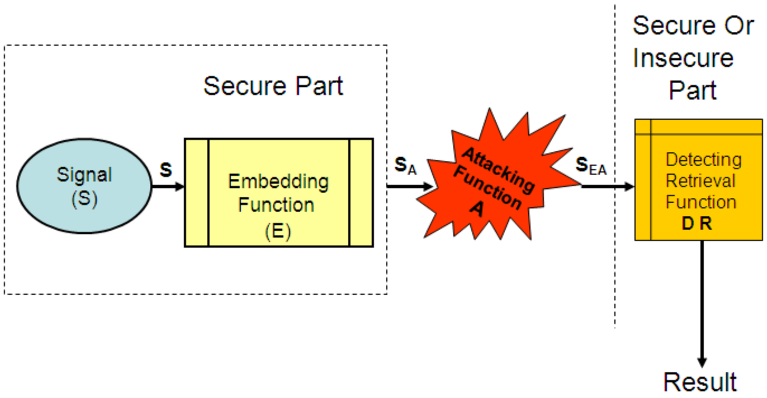

Figure N.2 Phases in digital watermarking.

As a next step, the watermarked digital signal is transmitted or stored – usually it is transmitted to another person. In case the recipient makes any change, it is called an *attack*. Although the changes made by recipient may not be malicious, the term attack is used because its use is in the context of copyright protection application, where "pirates," that is, perpetrators try removing the digital watermark by making alternations. Many forms of modifications are possible; for example, lossy compression of the data which results in low resolution, cropping an image or video or deliberately adding noise. "Extraction" or "Detection" is an algorithm and it is applied to the signal under attack to be able to retrieve the watermark from the signal. Suppose, the signal was not modified while it was being transmitted, then the watermark still would be present and therefore, it would be possible to extract it. When a digital watermarking application is "robust," it is possible to produce the watermark correctly by applying the extraction algorithm, even when the changes made are strong. On the other hand, when digital watermarking is "fragile" with the change made to the signal, extraction algorithm would fail.

When a visible digital watermark is prepared, the information can be in the picture or video format. The information is usually some text or a logo that is meant to identify the owner of the media/object (see Fig. N.1). As another example, consider a television broadcaster who adds his/her logo to the corner while transmitting video to make it appear as a visible watermark. In contrast to this, when an invisible digital watermark is prepared, although the information is added as digital data to audio, picture or video, it is not apparent as such. However, it may be possible to sense that some amount of information is hidden in the signal. The watermark may be incorporated to promote widespread use of the material/object. As such, it may be made easy to recover or, it may be a form of s where an entity sends a covert message hidden in the digital signal (recall discussion in Section 7.12 of Chapter 7). For both visible watermark as well as invisible watermark, the purpose is to affix the mark of possession or some descriptive information to the signal in a way that makes it hard to detach it. Use of hidden embedded information is possible as a means of secret communication between the parties.

The principle of watermarking is applied in copyright protection systems. These systems are meant to prevent or deter illegal copying of digital media. In this scenario, a copy device fetches the watermark from the signal prior to making a copy. The device takes a call whether to copy or not and that typically depends on what is contained in the watermark. Another application of digital watermarking is for the purpose of tracking a source. At each point of dissemination, a watermark is implanted into a digital signal. When a copy of the work is found later, the watermark may be obtained from the copy and that way, the source of the distribution becomes known. Supposedly, this technique has been used for detecting the source of illicitly copied movies.

From the discussion so far, we can understand that "digital watermarks" are characteristics of media that are added during production or distribution. Digital watermarks involve data that possibly has a steganographic way of getting embedded within the audio or video data. Given the great advantage from owners' perspective, digital watermarks can be used for a number of applications – for example, to record the distributor, to record the copyright owner, to identify the purchaser of the music, to record the distribution chain, for copyright protection, for source tracking (each recipient gets a different watermarked content), for broadcast monitoring (television news often contains watermarked video from international agencies) and for secret communication of messages to name a few application scenarios of digital watermark. It would be a fair statement to say that "digital watermarking" should be considered as a specialized form of "digital steganography."

In spite of their promise and technological complexity, "watermarks"' are not considered to be a full-DRM mechanism in their own right. Watermarks are used only as a component of a system for DRM, for example, as a help to provide trial evidence for only lawful avenues of rights management, rather than direct technological restriction. There are some programs for editing video and/or audio that may alter, delete or otherwise interfere with watermarks. There are some advanced programs or third-party media players that can make watermarking useless. To circumvent these challenges, new methods of detection are currently under investigation by both industry and non-industry.

DRM and Laws

The Digital Millennium Copyright Act (DMCA) is an extension to the US Copyright Law passed across the world on 14 May 1998, which levies criminal penalties on the production and distribution of technology that allows users to get around technical copy-restriction methods. Under the Act, by-passing a technological measure that effectively controls access to a work is illegal if done with the main objective of violating the rights of copyright holders. Systems tools and technologies employed for DRM have received some international legal support when the 1996 WIPO Copyright Treaty (WCT) was implemented. Article 11 of the Treaty requires enactment laws against DRM circumvention. Most member states of the World Intellectual Property Organization (WIPO) have implemented the WCT. The US implementation is the DMCA. By 2001 the treaty was implemented in Europe. There is a European directive on copyright – it mandates member states of the European Union (EU) to implement legal protections for technological prevention measures. The lower house of the French parliament, in 2006, adopted such legislation as part of the controversial DADVSI law; however, it added that protected DRM techniques should be made interoperable, a move which caused widespread controversy in the US.

Further Reading

Additional Useful Web References

1. You can read about DRM controversy and much more at: http://en.wikipedia.org/wiki/Digital_rights_management (29 December 2010).
2. RightManMD is a DRM product for mobile and desktop downloads, developed by STS Research – you can find more about the products at:
   http://rightman.in/ (29 December 2010).
3. The 2009 list of Top Countries in Piracy can be seen at:
   http://trak.in/tags/business/2010/05/12/software-piracy-india/ (6 September 2010).
   http://trak.in/tags/business/2010/05/12/software-piracy-india/ (6 September 2010).
4. The *Findings of the Fourth Annual Global PC Software Piracy Study* are released as a report by the Business Software Alliance (BSA), an international association representing the software industry. The report was seen at:
   http://tech2.in.com/india/news/stware/stware-piracy-in-india-drps-by-ne-percent:-study/5607/0 (6 September 2010).
5. To know more on India Software Piracy Scenario, visit:
   http://trak.in/tags/business/2010/05/12/software-piracy-india/ (6 September 2010).
   http://tech2.in.com/india/news/stware/stware-piracy-in-india-drps-by-ne-percent:-study/5607/0 (6th September 2010).
6. Asia Pacific Software Piracy Rates – see the link at:
   http://trak.in/tags/business/2010/05/12/software-piracy-india/ (6 September 2010).

7. KPMG Advisory *An Inconvenient Reality - The Unaccounted Consequences of Non-genuine Software Usage* can be read at:
http://www.in.kpmg.com/TL_Files/Pictures/An_Inconvenient_Reality.pdf (6 September 2010).

8. To know how digital watermarking works, visit:
http://www.google.co.in/imgres?imgurl=http://www.catchlock.com/2smile_watermark.png&imgrefurl=http://www.catchlock.com/how_it_works.php&usg=__UKOalaGq-Kz1--F7CbmFQLulJIM=&h=484&w=733&sz=395&hl=en&start=3&zoom=1&tbnid=r87R7sKJxQ14pM:&tbnh=93&tbnw=141&prev=/images%3Fq%3Ddigital%2Bwatermark%26hl%3Den%26gbv%3D2%26tbs%3Disch:1&itbs=1 (30 December 2010).

9. To know more about *Classification of Digital Watermarks*, interested readers may refer to:
http://deepaksharma.net/Documents/Watermarks%20Classification.doc and
http://www.authorstream.com/Presentation/aSGuest42523-368252-digital-watermark-bhu-dti-education-ppt-powerpoint/ (30 December 2010).

10. A power point presentation on digital watermarking is available at:
http://www.authorstream.com/Presentation/aSGuest42523-368252-digital-watermark-bhu-dti-education-ppt-powerpoint/ (27 December 2010).

11. A technical white paper on *Digital Watermarking Technology Overview* can be read at:
http://www.wipro.com/pdf_files/Digital_Watermarking_Tech_Overview.pdf (30 December 2010).

12. Read about attacks on digital watermarks at:
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=940053 (24 December 2010).
http://www.ee.sunysb.edu/~cvl/ese558/s2005/Reports/Abhishek%20Goswami/WatermarksByAbhishekGoswami.pdf (24 December 2010).

Book

1. Becker, E., Buhse, W., Günnewig, D. and Rump, N. (2003) *Digital Rights Management – Technological, Economic, Legal and Political Aspects*, Springer–Verlag, Germany