Category: Concepts, Trends and Challenges

Digital Rights Management for E-Content and E-Technologies

Yingge Wang
Wayne State University, USA

Qiang Cheng
Wayne State University, USA

Jie Cheng
Wayne State University, USA

Thomas S. Huang
University of Illinois at Urbana-Champaign, USA

INTRODUCTION

Digital rights management (DRM) provides digital content creators and owners with a range of controls over how their information resources may be used. It is a fairly young discipline yet is becoming increasingly important as digital content can be copied and distributed so easily that the piracy of them is growing critical. In addition, with the rapid adoption of the Internet as an e-content delivery channel, complex DRM systems are required to protect the digital content besides the distribution channel. Risking their intellectual property (IP) rights, many major e-content providers are relying on DRM to not only protect the packaged digital products, but also to promote the e-content market over the Internet.

As a multidisciplinary technology, DRM has advanced innovative research and development in various fields such as biometrics, watermarking, security protocols, smart-card technology, forgery detection, and secure collaboration and data sharing. Commercially, DRM provides the e-content market with a significant impetus to grow, where secure e-content distribution is essential. Despite its short history, many DRM tools have already been developed by IBM, Sony, Real Networks, Intertrust, and Thomson. These products need be compatible with existing standards for contents, consumer electronics, and often times, different DRM systems. Standardization efforts in industry are ongoing to ensure the interoperability of DRM products and services.

Another important impetus is the legal and regulatory framework. Technical measures provide an effective hurdle for limiting abuse, but legal actions against violators can prevent organized piracy from infringing. With a properly integrated legal, technological, and commercial framework, we expect that the DRM products and services will greatly foster the growth of the e-content market that is eagerly awaited by content providers and consumers. Without proper DRM technologies and laws, the creative industries that create digital products such as DVDs, business software, music recordings, theatrical films, and digital TV programs will suffer from piracy and would be reluctant to support Web-based commerce. The socio-economic impact of DRM is huge.

In this article, DRM techniques using cryptography, data hiding, and biometrics are discussed. Also covered are the standardization issues, emerging trends, and challenges in DRM-related technologies, commerce, and legislative regulations.

BACKGROUND

The beginning of DRM systems was in 1996 when the launch of the DVD raised copy protection concerns from the motion picture industry. The Copy Protection Technical Working Group (CPTWG) was created to address the copyright issues. CPTWG generated a series of commercial solutions, including the following.

- The content scrambling system (CSS) for DVDs in 1996
- Digital transmission content protection (DTCP) for securing compressed content across the IEEE 1394 interface in 1998
- High-bandwidth digital content protection (HDCP) for securing uncompressed content across the DVI (DVI, 1998) in 1999

Nowadays, e-technology providers, including IT and consumer electronics (CE) industries, produce DRM sys-

tems with respect to various e-business models. The interest in DRM comes from not only the copy protection of mass-distributed digital content like CDs and broadcast, but also from the promise of using the Internet as a content distribution infrastructure. Because DRM offers a means of setting up a contract between consumers and content providers, it can achieve much more restrictive and fine-grained usage rights than fair use defined by the U.S. Digital Millennium Copyright Act (DMCA, 2000).

Integrating Technological, Commercial, and Legal Measures

Technologically, encryption and watermarking are the pillars of most DRM systems. But they alone cannot prevent the systems from being attacked or circumvented. A serious vulnerability lies in key management. This may be addressed using biometrics for personal key generation or an additional layer of security in accessing the content.

We believe effective DRM systems should be based on a combination of technical means, legal agreements between the different parties, and the consumers' ability to access the digital data only on DRM-compliant devices. The concept of the compliance of devices refers to a common set of rules or policies agreed on by device manufactures, content producers, and consumers. This necessitates, among others, not only the regulation of the commercial activities of device manufacturers and e-content providers, but also the establishment of industrial standards governing the interoperability and behaviors of products and services.

Effective DRM systems should integrate technological measures, commercial products and services, business models, and legislative regulations. The interleaving of them shall enable the organic growth of DRM and thus the e-content market.

Legislative Aspects

The recognition and protection of IP rights is an international concern and effort. The World Intellectual Property Organization (WIPO), with 179 member states, enforces and protects IP around the world. Two WIPO treaties (1994, 1995) and other international treaties and conventions set up a complex framework invoking copyrights, neighboring rights, and exceptions. Correspondingly, most national laws recognize similar types of exceptions via restrictive lists or through general provisions. The DMCA (2000) lays the very legal foundation for DRM applications in United States. It defines an exception through fair use. Exceptions exempt certain uses of IP from authorization, but they are not rights. Thus, fair use needs to be enforced under the legal provisions as well as the agreement between content provider and consumers. The proper enforcement calls for technological protection means, and thus came DRM. Not only do legislative regulations lay the legal foundation for DRM techniques, but they also forbid tampering with the DRM technical barrier and severely punish violators (DMCA).

Despite the legislative efforts to protect copyrights, there are some challenges in the context of DRM systems to apply copyright laws. The foremost is due to underdeveloped policy languages and missing attributes. The copyrights are subject to a number of exceptions, which depend on a variety of factors including the user's role, intent, purpose of use, and so forth. A primary defense to a claim of infringement of fair use is fuzzy by nature. The risks of DRM systems must be examined due to automatic enforcement. There are some transactions between copyright holders and users that may benefit from the technical mechanisms; however, many legitimate, noninfringing uses of copyrighted works by individuals may be prevented. DRM systems often include authorization authorities from which the users are required to seek permission for the desired use. Virtually all DRM mechanisms utilize encryption for transport security, ensuring that the content is managed by a trusted agent. This may require users to divulge personal information prior to using a legally acquired copyrighted work at home, which is at odds with current consumer expectations.

Cryptographic Algorithms and Key Management for DRM

DRM technological tools usually consist of cryptographic algorithms, key management, watermarking, and personal authentication using biometrics. General security and privacy policies are often enforced with strong cryptographic algorithms, protocols, and key management. The cryptographic algorithms are used in DRM systems so that the consumers can only process the digital content on a trusted device. That is, the cryptographic algorithms in DRM prevent the consumers from accessing the digital data directly. A famous example is the CSS used for DVD encryption and key management. CSS provides a weak technical hurdle in its own right, with the effective encryption key length only in the order of 8 to 16 bits. Its protection primarily comes from the legal enforcement of DMCA. Also, the cryptographic algorithms provide a means to establish trust between consumers and device manufacturers. The management of trust needs to be handled be over time and across a huge number of devices. A famous example is the xCP technologies of IBM (Lotspiech, Nusser, & Pestoni, 2002), a peer-to-peer content-protection protocol utilizing Fiat and Naor's (1994)