DRM Technology for Mobile Multimedia

Sai Ho Kwok
California State University, Long Beach, USA

INTRODUCTION

Mobile multimedia has been promoted as a promising service and application in mobile e-commerce (m-commerce) by many mobile operators and mobile service providers, when high-speed mobile networks are expected to take off in the near future. However, at present, mobile multimedia is still in its infancy, accessed by relatively low-end mobile devices with limited bandwidth and resources. A typical example is Orange in Hong Kong which launched a low-grade multimedia service in 2000 to test the market with current mobile technologies. Due to the physical constraints of a 2.5G mobile network, audio broadcast is the best service that the network can offer up to date. However, in the near future, when advanced mobile networks and technologies become available, higher demands will be placed on the quality of mobile multimedia services. Such services support both audio and video data, for example, video conferencing, music video, video-on-demand and so on. Rights management deserves more serious concern because intellectual property of distributed multimedia content is as valuable as a company's physical assets (Doherty, 2002). This will become even more important when mobile multimedia services become marketable and an essential part of the business. The purpose of a digital rights management (DRM) system is to allow owners of digital assets (movies, songs) to distribute their products/services/contents electronically in a controlled way (Peinado, 2002). DRM technology makes various online payment schemes possible, such as pay-per-view, pay-per-download, pay-per-game and so on. Hence, mobile service providers are able to control end users' use of, and accessibility to, their products, and stand to gain huge profits from this capability with the DRM technology (Foroughi, Albin, & Gillard, 2002). A successful DRM system should address both business and technical issues (Grab, 2002), but this chapter only addresses and presents issues in the technical side due to the nature of this book. We present some critical issues of mobile DRM for mobile multimedia. A proposal of mobile DRM framework is presented to meet the urgent DRM needs with the existing 2.5G mobile technology. This chapter is concluded by presenting future directions of mobile DRM for mobile multimedia.

BACKGROUND

Internet Commerce

In the Internet domain, Vidius Incorporated estimates 450,000 to 580,000 downloads of unprotected full-length films are transferred over the Internet daily (Grab, 2002). Protection of distributed multimedia has been a growing concern to creators, distributors, copyright owners, publishers, and governments. DRM is considered to be one of the desirable solutions to this problem, and it can protect distributed media contents delivered over the Internet.

Several international standard organizations have been developing DRM solutions for various distributed multimedia, for example, digital music and video. The Secure Digital Music Initiative (SDMI) (SDMI, 2003), backed by the Recording Industry Association of America (RIAA) and 200 music and technology companies (as of October 2003), has been proposed to provide a secure environment for music distribution over the Internet. Another standard being developed by the Moving Picture Experts Group (MPEG) is known as MPEG-21 (Bormans & Hill, 2002) dedicated to distributing digital multimedia content. MPEG-21 defines an interoperable framework for Intellectual Property Management and Protection (IPMP). The IPMP can be interoperable with other MPEG standards, for example, MPEG-4. Therefore, the property protection will be also applicable to most of the MPEG video standards in the future. In addition, there are commercial DRM systems especially for the wired Internet business. They include Windows Media Rights Manager by Microsoft, and MetaTrust by InterTrust Technologies (InterTrust, 2000).

The above DRM standards and systems can be classified into two groups, namely, cryptographic-based and watermark-based DRM solutions (Kwok, 2003). Cryptographic systems permit only valid key-holders to access the encrypted data after receiving it from the authenticated senders. However, once such data is decrypted, it is impossible to track its reproduction or retransmission. Therefore, cryptography only provides protection during data transmission. Digital watermarking technology seems to complement the cryptographic process and to protect

Table 1. Summary of features of DRM solutions

• Media right protection and management • Secure delivery and distribution of digital contents • Processing authorization, data authentication and verification for content service • Data security, integrity check, access control, and management for distributed systems and peer-to-peer (P2P) networks • Multimedia watermarking for copyright protection, media authentication and integrity checking, finger-printing, and data annotation

Table 2. Problems and issues for mobile DRM

Mobile DRM standard: There is not yet a winner of mobile DRM standard. Open Mobile Alliance (OMA) DRM standard is one of the outstanding mobile DRM standards for mobile phones (Poropudas, 2003). However, other DRM standards, such as Windows Media DRM for Pocket PC (Microsoft, 2003), are highly competitive. **Trustful DRM protocol**: Since DRM involves many parties, for example, technology service providers, mobile operators, service providers, creators, distributors and so forth, trust may not exist in all of these parties, for example, in a second-hand market. Hence, a trustful DRM protocol that can deal with DRM but without assuming mutual trust between involved parties is needed. A similar protocol was proposed by Cheung and Curreem (2002). **Robust and secure watermarking**: A secure and robust watermarking algorithm is required to protect the distributed multimedia content. Such watermarking algorithm should resist attacks of any kinds. However, it cannot guarantee that a watermarking algorithm can resist all upcoming attacks (Tsang & Au, 2001). **Payment scheme**: When trust does not exist, for example, in the second-hand market, a reliable payment scheme becomes an important issue. **Rights expression language**: This is a need for a cross-platform rights expression language for all involved parties to specify and utilize their rights.

copyright ownership (Kwok, 2002). Digital watermarks can be visible but they are preferably invisible identification codes that are permanently embedded in the data and present within the data after any decryption process (Doherty, 2002).

In order to manage digital rights effectively and efficiently, many commercial DRM solutions employ license management models (Kwok & Lui, 2002). A license management model consists of a digital license that keeps access and control rights. Corresponding rights enforcement DRM applications determine usage rights based on these digital licenses.

Mobile Commerce

The current 2.5G mobile technologies for mobile multimedia service are fundamentally different from those used for Internet commerce service, and they impose many limitations and constrains upon the sophistication of mobile multimedia service. This explains why existing DRM systems for Internet commerce cannot be applicable to DRM over the mobile environment in a straightforward way. Some of the most important technical and physical obstacles are summarized as follows:

1. *License management:* A mobile device usually has limited resources of both memory and processing power to handle and process license documents and rights-protected contents.
2. *Limited storage and processing power:* Due to the limited resources of the mobile device, it is not possible to download rights-protected contents to the mobile device and play it there.