Chapter XXVII
Digital Watermarking for Digital Rights Management

Farid Ahmed
The Catholic University of America, USA

Cecilia Gomes
The Catholic University of America, USA

ABSTRACT

With the remarkable growth of Internet and multimedia applications, production and distribution of digital media has become exceedingly easy and affordable. Applications such as distance education, e-commerce, telemedicine, digital library, and live audio/video broadcast activities require distribution and sharing of digital multimedia contents. Consequently, maintaining the quality of service of the applications and the rights of the content owner as well as enforcing a viable business model among the producer, consumer, and distributor of digital contents has become an increasingly challenging task, leading to a contentious area called digital rights management (DRM). This chapter presents how digital watermarking (DWM) technology can addresses part of this DRM problem of secure distribution of digital contents

INTRODUCTION

The spectacular development in communication and network infrastructures coupled with exponential growth on digital contents and applications have placed enormous challenges on the storage, distribution, and use of these contents. The dissemination and sharing of information in this digital age consequently gives rise to a number of legal, ethical, and economic questions that need to be appropriately addressed by policy makers, consumers, developers, and technologists. We particularly address the technological aspect of the rights management of this digital distribution scenario in this chapter.

An analysis of the threat model, risks, and vulnerabilities associated with the storage and distribution of digital multimedia is first provided. Then we identify the requirements of enforcing the digital rights of different players, like the owner, distributor, and users involved in the transaction management of the digital contents. This leads to the design issues of different digital rights management (DRM) applications. Next, we specifically present a paradigm of technological solutions using the digital

watermarking (DWM) technology. A fairly moderate technical know-how of the digital watermarking technology will be presented to show how it can address the DRM problems in terms of copyright protection, copy protection, owner identification, content authentication, and transaction tracking. The effectiveness of the technology will be analyzed by defining a set of metrics derived from the requirements of multimedia distribution. Finally the limitations of DWM and interoperability with other technological solutions will be presented.

THE PROBLEM: THREATS AND VULNERABILITIES OF DIGITAL MULTIMEDIA DISTRIBUTION

Digital multimedia data are easy to share and copy. Most importantly the sharing and copying can be done without any distortion done to the contents. If some distortions occur, data can be reconstructed by various algorithms well-studied in the areas of digital communications and signal processing. Interestingly, this property of digital data that facilitates the easy distribution is also responsible for its misuse.

Digital representation of text, audio, speech, image, video, graphics, and animation fall in the general umbrella of digital multimedia. The continuation of the chapter will primarily focus on the rights management of digital images. Figure 1 shows the typical distribution of digital images. Data acquisition is performed using imaging sensors such as camera, radiography, ultrasonogram, electron microscope, and so forth.

Depending upon the use of the image, it can be processed thereafter for enhancement or filtering out sensor noises. It may then be consumed for its intended use, or it may leave the digital world to enter into the analog/print world. The image may go through some wear and tear processes in the print media, and after that it may be scanned back to digital form and eventually reconstructed back to its original quality. While in the digital form the images may be copied, shared, or distributed through digital media, networks, or Internet. In this life-cycle of a digital image, different players such as the creator, owner, distributor, buyer, seller, consumer, and user have different models of ownership rights. The ease of distribution coupled with different attack models has made the rights enforcement of digital data vulnerable. The vulnerabilities are manifested through copyright thefts, identity thefts, data piracy, unauthorized access, and counterfeiting (Stallings, 2003). In a networked environment, the threats and vulnerabilities to data are even more evident. Essentially, all sorts of digital data are at risk.

The Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) have jointly been conducting an annual survey of cyber-crimes for the last couple of years (CSI/FBI, 2007). It is

Figure 1. Life cycle of digital images