Chapter II
Secure Multimedia Content Distribution Based on Watermarking Technology

Shiguo Lian
France Telecom Research & Development–Beijing, P.R. China

ABSTRACT

Since the past decade, multimedia protection technologies have been attracting more and more researchers. Among them, multimedia encryption and watermarking are two typical ones. Multimedia encryption encodes media data into an unintelligible form, which emphasizes on confidentiality protection. Multimedia watermarking embeds information into media data, which can be detected or extracted and used to authenticate the copyright. Traditionally, in multimedia distribution, media data are encrypted and then transmitted, while the copyright information is not considered. As an important application, to trace illegal distributors, the customer information (e.g., customer ID) is embedded into media data, which can trace illegal distributors. In this chapter, the multimedia distribution scheme based on watermarking technology is investigated, which realizes both confidentiality protection and copyright protection. Firstly, some related works, including multimedia encryption and digital watermarking, are introduced. Then, the existing watermarking-based distribution schemes are reviewed and analyzed. Furthermore, the novel scheme is proposed and evaluated. Finally, some open issues are presented.

INTRODUCTION

With the development of multimedia technology and network technology, multimedia content becomes more and more popular in our lives. To keep security and privacy, multimedia content protection attracts more and more researchers. Generally, for multimedia data, the confidentiality and copyright are important properties that should be protected (Lin, Eskicioglu, Lagendijk, & Delp, 2005). Among them, confidentiality protection means to make only authorized users access mul-

timedia content, and copyright protection means to verify the ownership of multimedia content. To realize these functionalities, two means have been proposed, that is, digital watermarking and multimedia encryption.

Digital watermarking (Bloom et al., 1999; Hauer & Thiemert, 2004; Moulin & Koetter, 2005) embeds information (also named watermark) into multimedia data by modifying multimedia content slightly, which can also be detected or extracted from multimedia data. According to the visibility of the watermark, digital watermarking can be classified into two types, that is, visible watermarking and invisible watermarking. In visible watermarking, the embedded watermark is visible in multimedia data. In invisible watermarking, the watermark is imperceptible. Digital watermarking can be used for various applications (Cox, Miller, & Bloom, 2002), such as copyright protection, copy protection, transaction tracking, and so on. In copyright protection, the copyright information (e.g., ownership information) is embedded into multimedia content, which can be extracted and used to tell the ownership of the content. In copy protection, the permission information (e.g., copy times) is embedded into multimedia content, which can be modified according to copy operations. For example, if the original embedded copy time is 3, then after one copy operation, the embedded copy time is changed into 2. When the copy time becomes 0, copy operation is forbidden. As an important application, to trace illegal distributors, customer information, for example, customer ID, can be embedded into media data. Thus, each customer receives a slightly different copy, and the contained customer ID can be used to identify the customer. In this chapter, only the traitor tracing property is emphasized, and only the invisible watermarking is used here. In traitor tracing, some properties (Cox et al., 2002) should be satisfied, for example, robustness, imperceptibility, and security. Robustness denotes that the watermark can survive some intentional or unintentional operations, such as general signal processing (e.g., compression, adding noise, filtering, etc.) or intentional operations (e.g., camera capture, rotation, shifting, translation, etc.). Imperceptibility means that there is no perceptual difference between the watermarked multimedia content and the original content. Security denotes the ability to resist some attackers who forge the watermark or remove the watermark in an unauthorized manner.

Multimedia encryption (Lin et al., 2005; Maniccam & Nikolaos, 2004; Wu & Kuo, 2001) transforms multimedia content into an unintelligible form that can only be recovered by the correct key. Thus, for the authorized customer who has the key, the content can be recovered, while for the unauthorized customer who has no key, he/she can only watch the unintelligible content. As multimedia encryption algorithms, security is the most important requirement. Generally, as an encryption algorithm, it should be secure against such cryptographic attacks (Mollin, 2006) as brute-force attacks, statistical attacks, differential attacks, and so forth. Some detailed information about multimedia encryption will be presented in the second section.

Secure multimedia distribution is a practical application in multimedia communication, which transmits multimedia content from the sender to customers in a secure manner. Generally, both confidentiality protection and copyright protection should be confirmed. Thus, it is reasonable to adopt both multimedia encryption and digital watermarking techniques—for it implements both watermarking and encryption operations. The properties belonging to both watermarking and encryption should be satisfied, which are as follows:

- **Secure against cryptographic attacks.** The encryption algorithm should be secure against such attacks as brute-force attacks, statistical attacks, differential attacks, and so forth.