Chapter XVI
Multimedia Encryption and Watermarking in Wireless Environment

Shiguo Lian
France Telecom R&D Beijing, China

ABSTRACT

In a wireless environment, multimedia transmission is often affected by the error rate; delaying; terminal's power or bandwidth; and so forth, which brings difficulties to multimedia content protection. In the past decade, wireless multimedia protection technologies have been attracting more and more researchers. Among them, wireless multimedia encryption and watermarking are two typical topics. Wireless multimedia encryption protects multimedia content's confidentiality in wireless networks, which emphasizes on improving the encryption efficiency and channel friendliness. Some means have been proposed, such as the format-independent encryption algorithms that are time efficient compared with traditional ciphers; the partial encryption algorithms that reduce the encrypted data volumes by leaving some information unchanged; the hardware-implemented algorithms that are more efficient than software based ones; the scalable encryption algorithms that are compliant with bandwidth changes; and the robust encryption algorithms that are compliant with error channels. Compared with wireless multimedia encryption, wireless multimedia watermarking is widely used in ownership protection, traitor tracing, content authentication, and so forth. To keep low cost, a mobile agent is used to partitioning some of the watermarking tasks. To counter transmission errors, some channel encoding methods are proposed to encode the watermark. To keep robust, some means are proposed to embed a watermark into media data of low bit rate. Based on both watermarking and encryption algorithms, some applications arise, such as secure multimedia sharing or secure multimedia distribution. In this chapter, the existing wireless multimedia encryption and watermarking algorithms are summarized according to the functionality and multimedia type; their performances are analyzed and compared; the related applications are presented; and some open issues are proposed.

INTRODUCTION

With the development of multimedia technology and network technology, multimedia data are used more and more widely in human's daily life, such as mp3 sharing, video conference, video telephone, video broadcasting, video-on-demand, p2p streaming, and so forth. For multimedia data may be in relation with privacy, profit, or copyright, multimedia content protection becomes necessary and urgent. It permits that only the authorized users could access and read the multimedia data, it can detect the modification of the multimedia data, it can prove the ownership of the multimedia data, it can even trace the illegal distribution of the multimedia data, and so forth.

During the past decades, some means have been proposed to protect multimedia data. Among them, multimedia encryption (Furht & Kirovski, 2006) and multimedia watermarking (Cox, Miller, & Bloom, 2002) are two typical ones. Multimedia encryption algorithms protect multimedia data's confidentiality by encoding or transforming multimedia data into unintelligible forms under the control of the key. Thus, only the authorized users who have the correct key can recover the multimedia data successfully. Till now, some multimedia encryption algorithms have been proposed, which focus on the security, time efficiency, and communication friendliness (Zeng, Zhuang, & Lan, 2004). Multimedia watermarking algorithms protect multimedia data's ownership by embedding ownership information into multimedia data under the control of the key. Thus, the authorized users can extract or detect the ownership information and authenticate it. Many watermarking algorithms (Barni & Bartolini, 2004) have been proposed during the last decade, which consider security, imperceptibility, robustness and capacity, and so forth.

Recently, mobile/wireless multimedia communication has become more and more popular, which benefits from the improvement of the capability of mobile terminals and the bandwidth of wireless channel. Compared with wired communication, wireless multimedia communication has some special properties (Salkintzis & Passas, 2005). Firstly, the bandwidth is still limited compared with wired channels. Secondly, there are many more transmission errors in wireless communication, such as channel error, loss, delay, jitter, and so forth, which are caused by path error, fading, noise or interference, and so forth. Thirdly, wireless or mobile terminals are often of limited memory. Fourthly, the terminals are often energy-constraint caused by the scale-limited battery. These properties push some requirements to multimedia encryption and watermarking algorithms.

To meet mobile/wireless multimedia content protection, some mobile digital rights management (DRM) systems (Kundur, Yu, & Lin, 2004) have been proposed, such as Nokia's Music Player, NEC VS-7810, Open Mobile Alliance (OMA), and so forth. In these systems, multimedia encryption and multimedia watermarking are two core technologies. Compared with wired environment, wireless multimedia encryption and watermarking should consider some extra requirements. For example, the algorithms should be lightweight in order to meet the constraint energy of the terminals. Additionally, the algorithms should be robust against transmission errors in some extent. Furthermore, the algorithms should be scalable to switch between wireless services and wired services.

During the past decade, some means have been proposed to make suitable wireless multimedia encryption and watermarking algorithms. These algorithms obtain the security, efficiency, and error robustness by considering the properties of wireless/mobile multimedia communication. In this chapter, they are classified into several types according to the functionalities, and their performances are analyzed and compared. Additionally, some open issues are presented.

The rest of the chapter is arranged as follows. In the next section, the requirements of wireless/mobile multimedia encryption and watermarking are presented respectively. The multimedia encryption algorithms are analyzed and compared in the third section, and the watermarking algorithms are analyzed and compared in the fourth section. In the fifth section, some research topics and applications based on the combination of watermarking and encryption are presented, followed by some