Chapter XXX
Traitor Tracing in Mobile Multimedia Communication

Shiguo Lian
France Telecom R&D Beijing Center, China

ABSTRACT

Digital fingerprinting is reported and used in copy tracing. It embeds different information, for example, Customer ID, into multimedia content, produces a different copy, and sends the copy to the corresponding customer. If a copy is spread to unauthorized customers, the unique information in the copy can be detected and used to trace the illegal distributors. In this chapter, we introduce some digital fingerprinting algorithms, review the existing traitor tracing schemes, analyze the performances of some typical algorithms through comparison, and propose the future trends and some open issues in this field. It is expected to provide some valuable information to researchers or engineers working in mobile multimedia security.

INTRODUCTION

With the advances in mobile multimedia technology, multimedia content (e.g., image, audio, video, flash, game, etc.) becomes more and more popular in human's daily life, such as the applications of short message sending (SMS), multimedia message sending (MMS), ring-tone, mobile TV, and so on. In multimedia-related applications, digital rights management (DRM) (Kundur, Yu & Lin, 2004) is necessary and urgent, which protects not only the ownership, confidentiality and integrity of multimedia content but also the rights of content producer or service provider.

Till now, some DRM systems have been reported, such as Open Media Alliance (OMA), Internet Stream Media Alliance (ISMA), Advanced Access Content System (AACS), and so forth. Among them, OMA provides the open DRM standard for mobile multimedia. In this standard, the encryption algorithms (Furht & Kirovski, 2006) are used to protect the content's confidentiality, the authentication methods (Ho & Li, 2004) are used to confirm the content's in-

tegrity, and watermarking technique (Cox, Miller & Bloom, 2002) is used to protect the content's ownership. The encryption algorithms transform multimedia content into an unintelligible form. Differently, authentication methods generate an authentication code from multimedia content and use it to detect whether the content is changed or not. The watermarking technique embeds some information (e.g., ownership, content ID, content title, etc.) into multimedia content by modifying the content slightly, which is later extracted from the embedded content and used to tell the ownership information.

With the development of multimedia technology, multimedia signal processing becomes easier and easier, such as capturing, storing, displaying or manipulating. Multimedia content distribution often faces such a problem, that is, a customer may redistribute the received content to other unauthorized customers. The customer who redistributes the content is called the traitor. This typical problem often causes great profit-losses of content provider or service provider.

As a potential solution, digital fingerprinting (Wu, Trappe, Wang & Liu, 2004) is recently reported and studied. It embeds different information, such as Customer ID, into multimedia content, produces a unique copy, and sends the copy to the corresponding customer. If a copy is spread to unauthorized customers, the unique information in the copy can be detected and used to trace the illegal redistributor. It seems a good solution. However, another question arises, that is, different customer combines different copy through averaging or some other operations to produce a new copy, which is named collusion attack (Wu et al., 2004). For there is often few differences between these copies, the collusion operation may make the embedded information lost. This kind of attack is named collusion attack. Since the past decade, finding new solutions resisting collusion attacks has been attracting more and more researchers.

In this chapter, we introduce some digital fingerprinting algorithms, review the existing traitor tracing schemes based on digital fingerprinting, analyze the performances of some typical algorithms through comparison, and propose the future trends and some open issues in this field. It is expected to provide some valuable information to researchers or engineers working in mobile multimedia security.

The rest of chapter is arranged as follows. In the Background section, we introduce the watermarking technique that is the basic of digital fingerprinting. Collusion attacks and some digital fingerprinting algorithms are introduced in the Collusion Attacks section and the Typical Fingerprinting Algorithms section, respectively. In Secure Fingerprint Embedding section, we review the existing traitor tracing schemes based on digital fingerprinting. The future trends and some open issues are proposed in the Open Issues and Future Trends section . Finally, we finish with a Conclusions section.

BACKGROUND

Digital fingerprinting embeds the unique information, such as customer ID, into media content with the watermarking technology. Thus, digital watermarking is the basic of digital fingerprinting, which is introduced in this section.

Digital watermarking protects 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 (Cox et al., 2002; Barni & Bartolini, 2004; Petitcolas, Anderson & Kuhn, 1999; Linnartz & Dijk, 1998; Kutter, Volosphynovskiy & Herrigel, 2000) have been proposed during the last decade. Generally, for digital watermarking, some performances are required, such as security, robustness, transpar-