Chapter XV
Traitor Tracing for Multimedia Forensics

Hongxia Jin
IBM Almaden Research Center, USA

ABSTRACT

This chapter discusses the cryptographic traitor tracing technology that is used to defend against piracy in multimedia content distribution. It talks about different potential pirate attacks in a multimedia content distribution system. It discusses how traitor tracing technologies can be used to defend against those attacks by identifying the attackers involved in the piracy. While traitor tracing has been a long standing cryptographic problem that has attracted extensive research, the main purpose of this chapter is to show how to overcome many practical concerns in order to bring a theoretical solution to practice. Many of these practical concerns have been overlooked in academic research. The author brings first-hand experience on bringing this technology to practice in the context of new industry standards on content protection for next generation high-definition DVDs. The author also hopes to shed new insights on future research directions in this space.

INTRODUCTION

Today we live in a digital world. The advent of digital technologies has made the creation and manipulation of multimedia content simpler. It offers higher quality and a lot more convenience to consumers. For example, it allows one to make perfect copies.

Furthermore, the rapid advance of network technologies, cheaper storage, and larger bandwidth have enabled new business models on electronically distributing and delivering multimedia content, such as Disney's MovieBeam and Apple's iTune.

However, unauthorized music and movie copying are eating a big bite of the profit of the record industry and the movie studios. The success of these emerging business models hinges on the ability to only deliver the content to paying customers.

It is highly desirable to develop better techniques to protect the copyrighted material.

Content encryption solves part of the problem. It protects the content before and during delivery, but does not help after it has been decrypted. It is relatively easy for hackers to access the content after decryption. To protect the copyright of the content, one must also ensure that content is only consumed by authorized users.

Digital fingerprinting are unique labels/marks embedded in different copies of the same content. When an illegal copy of the post-delivery multimedia content is found, the embedded fingerprint can be used for tracing the illegal users who distributed that copy.

Of course there are different pirate attacks. The piracy may not be on content; it can also be on the decryption keys of the content. Fingerprinting technology usually does not apply to cryptographic keys.

The focus of this chapter is not on content fingerprinting, instead it is on *traitor tracing*.

Before we go on in this chapter, we need to first clarify the terminology traitor tracing.

People working on multimedia have been using the terminology traitor tracing meaning the function/capability that traces traitors. So one can say fingerprinting is a technology that can be used for traitor tracing. However, traitor tracing is also a terminology that has been actively appeared in cryptographic literatures. It refers to a class of key management schemes that can be used to trace pirated cryptographic keys, sometimes pirated content too. To this end, traitor tracing itself is a technology that can be used for forensics, including multimedia forensics. The focus of this chapter is on the latter cryptographic traitor tracing technology, which has been and still is a very active research area in cryptographic community.

In this chapter, we will describe different pirate attacks. We will survey the state of art and state of practice of the traitor tracing technologies for different pirate attacks. Different traitor tracing technologies are needed for different types of pirate attacks. The author and colleagues have been involved in this research area for many years. The technologies they developed have become the first large scale commercialization of traitor tracing technologies in the context of new industry content protection standard, the advanced access content system (AACS), for next generation high definition DVDs. In this chapter the author will describe their first hand experience on developing traitor tracing technologies that are practical enough for commercial use. The focus of this chapter is from a practical point of view looking at the problems and how researches can be done to make the technologies work in practice. It will give readers hands on knowledge on using traitor tracing technologies for multimedia forensics in different types of pirate attacks in real world. This chapter will also point out some of the issues that have been overlooked in years of academic researches.

BACKGROUND

A number of business models have emerged, whose success hinges on the ability to securely distribute digital content only to paying customers. Examples of these business models include pay-TV systems (Cable companies) or movie rental companies like Netflix, and massively distributing prerecorded and recordable media. These typical content protection applications imply a one-way broadcast nature. To ensure the content is only consumed by authorized users, broadcast encryption technologies are used.

A broadcast encryption system (Fiat & Naor, 1993) enables a broadcaster to encrypt the content so that only a privileged subset of users (devices, set up boxes) can decrypt the content and exclude another subset of users. In this system, each decoder box is assigned a unique set of decryption keys (called device keys). A key management algorithm is defined to assign keys to devices and