Chapter XVI
Forensic Watermarking for Secure Multimedia Distribution

Farook Sattar
Nanyang Technological University, Singapore

Dan Yu
Hewlett-Packard, Shanghai, China

ABSTRACT

This chapter discusses on forensic tracking through digital watermarking for secure multimedia distribution. The existing watermarking schemes are elaborated and their assumptions as well as limitations for tracking are discussed. Especially, an Independent Component Analysis (ICA) based watermarking scheme is presented, which overcomes the problems of the existing watermarking schemes. Multiple watermarking techniques are used where one watermark is used for ownership verification and the other one is used to identify the legal user of the distributed content. In the absence of a priori information, i.e. the original data, original watermark, embedding locations as well as the strength, our ICA technique provides efficient watermark extraction scheme with the help of side information. The robustness against common signal processing attacks is presented. Lastly, the challenges in the forensic tracking through digital watermarking techniques are discussed.

INTRODUCTION

In recent years, there has been enormous growth in multimedia technologies and computer network. Thus, the distribution of digital multimedia such as audio, image, video, text have become quite easy through various communications media e.g. *Internet.* It has a world-wide broadcasting capability, a mechanism for information distribution, and a medium for collaboration and interaction between individuals and their computers irrespective to geographic location. This allows researches and professionals to share the relevant data, information with each other.

As image, audio, video and other works become available in digital form, it may be ease for some

one to make perfect copies of the multimedia data. The widespread use of *Internet* have added substantially an astonishing abundance of information in digital form, as well as offering unprecedented ease of access to it. Creating, publishing, distributing, using, and reusing information have become much easier and faster in the past decade. The good news is the enrichment that this explosive growth in information brings to society as a whole. The bad news is the enrichment that it can also bring to those who take advantage of the properties of digital information and the Web to copy, distribute, and use information illegally. The Web is an information resource of extraordinary size and depth, yet it is also an information reproduction and dissemination facility of great demand and capability. Therefore, there has been currently significant amount of research in intellectual property protection issues involving the multimedia content distribution through *Internet*.

Thus the aim of this chapter is to present the forensic tracking through digital watermarking. An Efficient Independent Component Analysis (ICA) based watermarking technique is applied for watermark extraction in order to verify the authorized user of the distributed content, and hence to do the forensic tracking of the multimedia data to be protected.

MULTIMEDIA DISTRIBUTION STRATEGY THROUGH DIGITAL WATERMARKING

The rapid growth of networked multimedia systems has increased the need for the protection and enforcement of intellectual property (IP) rights of digital media. The IP protection for multimedia distribution in the *Internet* can be elaborated as follows:

- **Ownership identification:** The owner of the original Work must be able to provide the trustful proof that he/she is the rightful owner of the content.
- **Transaction tracking:** The owner must be able to track the distributions of the Work, so that he/she is able to find the person who should be responsible for the illegal replication and re-distribution.
- **Content authentication:** The owner should be able to detect any illegal attempts to alter the Work.

This chapter concentrates on the task of forensic tracking for multimedia distribution applications. Let consider the scenario when an owner would like to sell or distribute the Work for the registered users only. To enforce the IP rights, two primary problems are to be solved. First of all, the owner needs to prove that he/she is the legal owner of the distributed content. Secondly, if the data have been subsequently copied and redistributed illegally, how it is possible for the owner to find the person who is responsible for the illegal copying and redistribution of the data (see Figure 1).

The first technology adopted to enforce protection of IP rights is the cryptography. The cryptographic technology (Schneier, 1995) provides an effective tool to secure the distribution process and control the legal uses of the contents that have been received by an user. The content to be delivered in the Internet is encrypted, and only the legal users who hold the decryption key are able to use the encrypted data whereas the data stream would be useless to a pirate without the appropriate decryption key. However, for the error-free transmission through a network, the contents after the decryption in the cryptography will be exactly the same as the original data. The data contents can be replicated perfectly as many times and the user can also manipulate the contents.

Researchers and scientists are then turned to search for other technologies to counter copyright piracy on the global networks that are not