Chapter 8.2
Copyright Protection in Virtual Communities through Digital Watermarking

Huayin Si
University of Warwick, UK

Chang-Tsun Li
University of Warwick, UK

INTRODUCTION

Although the development of multimedia processing techniques has facilitated the enrichment of information content, and the never-ending expansion of interconnected networks has constructed a solid infrastructure for information exchanges, meanwhile, the infrastructure and techniques have also smoothed the way for copyright piracy in virtual communities. As a result, the demand for intellectual property protection becomes apparent and exigent. In response to this challenge, digital watermarking has been proposed to serve this purpose.

The idea of digital watermarking is to embed a small amount of secret information—the watermark—into the host digital productions, such as image and audio, so that it can be extracted later for the purposes of copyright assertion, authentication and content integrity verification, and so forth. Unlike traditional watermarks printed on paper, which are visible to human eyes, digital watermarks are usually invisible and can only be detected with the aid of a specially designed detector. One characteristic distinguishing digital watermarking from cryptography, which separates the digital signature from the raw data/content, is that digital watermarking embeds the signature in the content to be protected. The superiority of this characteristic is that while cryptography provides no protection after the content is decrypted, digital watermarking provides "intimate" protection, because the digital signature/secret information has become an inseparable constituent part of the content itself after embedding. Because of the very characteristic, digital watermarking requires no secret channel for communicating the digital signature that cryptography does. So in the last decade, digital watermarking has attracted numerous attention from researchers and is regarded as a promising technique in the field of information security.

Various types of watermarking schemes have been developed for different applications. According to their natures, digital watermarking schemes could be classified into three categories: *fragile* watermarking, *semi-fragile* watermarking and *robust* watermarking. The schemes of the first two categories are developed for the purposes of multimedia authentication and content integrity verification, in which we expect the embedded watermark to be destroyed when attacks are mounted on its host media. More emphases of these schemes are placed on the capability of detecting and localizing forgeries and impersonations. The main difference between the two is that semi-fragile watermarking is tolerant to non-malicious operations, such as lossy compression within a certain compression ratio, while fragile watermarking is intolerant to any manipulations. Robust watermarking, on the other hand, is intended for the applications of copyright protection, wherein the watermarks should survive attacks aiming at weakening or erasing them provided the quality of the attacked content is still worth protecting. Therefore, the emphasis of robust watermarking schemes is placed on their survivability against attacks.

This article is intended to focus on robust watermarking schemes for the application of copyright protection. See Li and Yang (2003) and Lin and Chang (2001) for more details about fragile and semi-fragile schemes.

ROBUST WATERMARKING APPROACHES

Robust watermarking is applicable in the areas of copyright protection such as ownership identification/proof, copy control/copy prevention, fingerprinting/transaction tracking and so forth. Some common requirements for the robust watermarking schemes are:

- **Transparency:** The watermark should be invisible to human perception after embedded in the host media, so the impact on the perceptual quality is minimized.
- **Robustness:** Survivability against all kinds of malicious attacks and incidental manipulations, such as lossy compression and format trans-coding, should be maintained unless the manipulations have rendered the content useless in some sense.
- **Payload:** Payload (i.e., the embedding capacity) is important for applications such as "traitors" tracing. To trace the origin of pirated copies, unique secret information that identifies the recipient/buyer for each original copy has to be embedded when purchased. To avoid collusion of a number of buyers, such schemes should provide enough capacity to contain the information. Detailed treatment on collusion attack can be found in Trappe, Wu, Wang and Liu (2003).
- **Computing Complexity:** Complexity is expected to be low enough to enable online and real-time watermarking or detecting, especially for mobile devices without the aid of a computer.

These requirements are so conflicting that no watermarking scheme can provide a cure-