Digital Watermarking for Multimedia Security Management

Chang-Tsun Li
University of Warwick, UK

INTRODUCTION

The availability of versatile multimedia processing software and the far-reaching coverage of the interconnected networks have facilitated flawless copying and manipulations of digital media. The ever-advancing storage and retrieval technologies also have smoothed the way for large-scale multimedia database applications. However, abuses of these facilities and technologies pose pressing threats to multimedia security management in general, and multimedia copyright protection and content integrity verification in particular. Although cryptography has a long history of application to information and multimedia security, the undesirable characteristic of providing no protection to the media once decrypted has limited the feasibility of its widespread use. For example, an adversary can obtain the decryption key by purchasing a legal copy of the media but then redistributing the decrypted copies of the original.

In response to these challenges, digital watermarking schemes have been proposed in the last decade. The idea of digital watermarking is to embed a small amount of imperceptible secret information in the multimedia so that it can be extracted later for the purposes of copyright assertion, copy control, broadcasting, authentication, content integrity verification, and so forth. For example, a stream of binary bits generated, which identifies the owner of an image, can be taken as a watermark embedded at the least significant bit of the pixels or transformed coefficients by adjusting their value according to a predefined algorithm. Since the secret information is embedded in the content of the media, for the applications related to copyright protection where the watermark is intended to be robust, it does not get erased when the content is manipulated or undergoes format conversions. In this article, we will be addressing the main applications, security issues/challenges, solutions, and trends in the development of digital watermarking schemes. Bearing in mind that providing a comprehensive coverage of the applications, issues, and approaches of digital watermarking is not realistic due to the length limitation, we will refer the reader to some most recent publications in due course.

BACKGROUND

Unlike traditional watermarks on paper, which are visible to the eyes, digital watermarks can be designed to be imperceptible and removable. Throughout the rest of this article, the term *watermark*(*ing*) is used to refer to digital watermark(ing).

Various types of watermarking schemes have been proposed for different applications. For copyright-related applications, the embedded watermark is expected to be immune to various kinds of malicious and non-malicious manipulations to some extent, provided that the manipulated content is still valuable in terms of commercial significance or acceptable in terms of perceptual quality. Therefore, watermarking schemes for copyright-related applications are typically robust (Barni et al., 2002; Moulin & Ivanovic, 2003; Sebe & Domingo-Ferrer, 2003; Trappe et al., 2003); that is, they are designed to ignore or remain insensitive to manipulations.

Conversely, in medical, forensic, and intelligence or military applications, where content integrity and source authentication are a major concern, more emphases are placed on the schemes' capability of detecting forgeries and impersonations. Therefore, schemes of this type are usually fragile or semi-fragile and are intended to be intolerant to manipulations (Barreto et al., 2002; Li, 2004a; Li & Yang, 2003; Wong & Memom, 2000; Xie & Arce, 2001). Although a watermark is designed to be imperceptible to humans, the embedding is certainly intrusive and incurs distortion to the content.

In some authentication applications where any tiny changes to the content are not acceptable, the embedding distortion has to be compensated for perfectly.

In an attempt to remove the watermark so as to completely recover the original media after passing the authentication process, reversible watermarking schemes have been proposed in the last few years (Alattar, 2004; Fridrich et al., 2002; Li, 2004b; Tan, 2003).

Requirements of digital watermarking vary across applications. The main requirements are low distortion, high capacity, and high security. One issue is that meeting all the three requirements simultaneously is usually infeasible; thus, trade-offs are frequently made to optimize the balance for each specific application. In many applications, where original media are not available at the watermark decoder, blind detection of the watermark without any prior knowledge about the original is desirable.

WATERMARKING SCHEMES AND THEIR APPLICATIONS

Digital watermarking schemes can be broadly classified into four categories: robust, fragile, semi-fragile, and reversible. While imperceptibility, low embedding distortion and security are the common requirements of all classes, each different category of scheme has different characteristics and, thus, is suitable for different applications. For example, while robustness is an essential requirement for copyright applications, it has no role in most authentication applications.

Robust Watermarking Schemes

Watermarks of robust schemes are required to survive manipulations, unless they have rendered the content valueless in some sense. This class of schemes has found its applications in the following areas. (The reader is reminded that the following list is not intended to be exhaustive, but just to identify some possible applications of multimedia security management.)

- **Ownership Proof and Identification:** A watermark containing the identification information of the content owner can be embedded in the host media for proving or identifying copyright ownership. However, proving ownership requires a higher level of security than ownership identification. For example, as pointed out by Craver et al. (1998), Bob could embed his watermark or make it appear that his watermark were embedded in a media owned and watermarked by Alice and could claim that this media belongs to him. In this scenario, the media contains both watermarks of Bob and Alice. Possible solutions to this problem of ambiguous ownerships have been reported in Craver et al. (1998) and Liu and Tan (2002).
- **Transaction Tracking/Fingerprinting:** The copyright owner could insert a unique watermark, which, for example, identifies the recipient, into each copy of the media and use it to trace the source, should illegal redistribution occur. The main challenge fingerprinting schemes face is the so-called *collusion attack* in which several legal copies of the same media are obtained to produce an approximation of the original unwatermarked version for illegal redistribution. Some recent proposals for tackling collusion attack can be found in Trappe et al. (2003) and Sebe et al. (2003).
- **Copy Control/Copy Prevention:** Illegal copying or recording is another common piracy scenario. One possible solution is to embed a never-copy watermark, which, when detected by the detector installed in the recording device, disallows further recording. However, this mechanism requires every recording device to have a watermark detector. It is difficult to persuade consumers to pay more for a device that restricts their freedom to make copies. This commercially undesirable requirement is unlikely to be met without the support of global legislation. The reader is referred to Bloom et al. (1999) for more details.
- **Broadcast Monitoring:** In advertisement applications, by embedding a watermark that is to be broadcast along with the host media, the advertisers can monitor whether or not the commercials they have paid for are aired by the broadcasters according to the contracts. More details can be found in De Strycker et al. (2000).

There are two major approaches to the designing of robust watermarking schemes; namely, spread spectrum (SS) watermarking (Cox et al., 1997) and

Maxout Networks for Visual Recognition
Gabriel Castaneda, Paul Morrisand Taghi M. Khoshgoftaar (2019). *International Journal of Multimedia Data Engineering and Management (pp. 1-25).*
www.irma-international.org/article/maxout-networks-for-visual-recognition/245261