Chapter 19
Multimedia Copyright Protection Scheme Based on the Direct Feature-Based Method

Rimba Whidiana Ciptasari
Kyushu University, Japan & Telkom Institute of Technology, Indonesia

Kouichi Sakurai
Kyushu University, Japan

ABSTRACT

This chapter discusses the direct feature-based method as an alternative approach to digital watermarking. Fundamentally, the direct feature-based method is an extension of the digital signature scheme, which aims at multimedia authentication. The method covers several copyright protection properties, i.e., robustness to content manipulations and sensitivity to content modification. In addition, this method provides solutions to inherent problems that arise in traditional watermarking, such as quality degradation, the trade-off between data payload, and imperceptibility or robustness.

Researchers have devised the direct feature-based method to improve traditional digital watermarking whilst developing the copyright protection scheme. A discussion on various multimedia copyright protection schemes based on the direct feature-based method (e.g., image, audio, text document, geospatial data, and relational databases) follows. In conclusion, the authors show that a good copyright protection scheme should not only be robust enough to endure acceptable manipulations, but also secure enough to withstand malicious attacks. In addition, the direct feature-based method can be considered a viable solution to the trade-off between data payload, fidelity, and robustness.

DOI: 10.4018/978-1-4666-2217-3.ch019
INTRODUCTION

The art of data hiding, which is embedding data inside a host medium without substantially altering it, is used in copyright protection. In 2003, direct feature-based extraction was proposed as another approach in the field of multimedia copyright protection. The direct feature-based method, an extension of the digital signature scheme, was ostensibly intended for the purpose of multimedia authentication. The premise of this development accommodates the need for copyright protection, i.e. an ability to withstand content manipulations and sensitivity to content modification. Therefore, several researchers have incorporated these properties into copyright protection.

One branch of research has led to the development of a copyright protection scheme (based on the direct feature-based method) known as zero-watermarking, although this is not widely known to those unfamiliar with the scheme. However, this term is most commonly used when the host medium is not changed during the embedding process. Researchers with an interest in cryptography meanwhile, strenuously argue that zero-watermarking should not be considered as watermarking since the host medium is not affected. While such distinction may be valid, the schemes presented in this chapter mainly focus on the zero-watermarking scheme. However, to avoid misinterpretation, zero-watermarking is hereby termed “DeFeat-based method,” which refers to the copyright protection scheme based on the direct feature-based method. Where necessary, the term zero-watermarking and DeFeat-based method may be used interchangeably for a particular purpose.

In summary, this chapter has several objectives: (1) to define the scope of the copyright protection scheme based on a DeFeat-based extraction; (2) to discuss briefly the fundamental knowledge used in the DeFeat-based extraction; (3) to describe state-of-the-art of multimedia copyright protection based on DeFeat-based extraction; (4) to provide a summary on the performance of the DeFeat-based method in terms of robustness and security.

BACKGROUND

Copyright protects the author’s original work against plagiarism and the distribution, commercial or otherwise, of unauthorized reproductions. The use of the Internet has resulted in the ease of copying digital information without any loss of quality. This has a considerable impact on the originators and owners of intellectual property. To solve the problem of publishing digital multimedia, researchers have come up with digital image watermarking. This method allows the owner of an original image to add an invisible watermark to the digital image before publishing it. The watermark serves to enforce copyright on the image. The owner protects the watermark with a cryptographic secret key in order to prevent an unauthorized party from reading or even detecting the watermark. The watermark is also designed to be robust against image tampering. Therefore, anyone who wants to distribute the image further will also distribute the watermark with it, which implies that they will have violated the copyright of the image. If the copyright holder can detect the fraud, he/she can prove ownership by showing that the image contains his/her proper private watermark.

The protection of the creators’ work encompasses many different aspects including copyright protection and moral rights protection. We examine three types of watermarking applications dealing with Intellectual Property Right (IPR) protection (Barni & Bartolini, 2004).

Rightful Ownership

The owner wishes to prove that he/she is the only legitimate owner of the work. To do so, as soon as he/she creates the work, he/she embeds