Chapter 14
Self-Embedding Watermarking with Content Restoration Capabilities

Rong Huang
Kyushu University, Japan

Kyung-Hyne Rhee
Kyushu University, Japan & Pukyong National University, Korea

ABSTRACT
In this chapter, the authors give a survey about self-embedding watermarking, which enables not only detection of tampered regions but also recovering the damaged information. They introduce the pioneering method as well as the representative schemes, including adjacent-block detection, hierarchical detection and self-recovery, dual watermarks, reference sharing, and flexible self-recovery. The authors analyze the distinguishing features and loopholes by considering four key techniques, namely the secure block-mapping function, the unambiguous authentication, the reference information extraction, and the watermark embedding approaches. They make comparative studies on the above works and then outline further research directions and a conclusion.

1. BACKGROUND

With the proliferation of the sophisticated and powerful digital image processing software, such as PhotoShop, PaintShop, and FreeHand, tampering images becomes easier even for an amateur. As a result, those tools threaten to diminish the credibility of digital images. Professor Hany Farid warns that we are living in a world where seeing (or hearing) is no longer believing. The severe situation has spurred a great deal of intensive research activities in the study of multimedia security. Several concepts such as image encryption, steganography, watermarking, signature, and blind/passive, forensic and corresponding methods have been proposed as a protection against illegal access to private information or as means for authentication and tampering detection. For
Self-Embedding Watermarking with Content Restoration Capabilities

Ease of exposition, in this chapter, we assume that the target being protected is a still image, although there exist a great many multimedia security techniques designed for audio (Kirovski & Malvar, 2003; Wang & Zhao, 2006; Wu, et al., 2005) and video data (Bloom, et al., 1999; Doerr & Dugelay, 2003).

Generally speaking, encryption techniques (Chen, Mao, & Chui, 2004; Cheng & Li, 2000; Wu & Kuo, 2005) transform the original image to a non-recognizable form under the control of key while steganography techniques (Chang, Chen, & Lin, 2004; Lee, et al., 2008; Marvel, Boneclet, & Retter, 1999; Petricolas, Anderson, & Kuhn, 1999; Tsai, Hu, & Yeh, 2009) hide the existence of one target image through embedding itself to the cover/host image. Of course, the above two types of techniques are not independent. Obviously, a designer can combine them by implementing encryption prior to embedding for enhancing the security. The common objective of encryption and steganography is to protect the target image’s information from being stolen by the eavesdropper.

On the other hand, watermarking, signature and blind/passive forensic focus on authentication and tampering detection. Watermarking (Celik, et al., 2002; Cox, et al., 1997; Hartung & Kutter, 1999; Thodi & Rodriguez, 2007) can be considered as an active and invasive technique. Here, we use term “active” to indicate that the watermark should be embedded by the sender and must be present in the host image before the tampering occurs, while invasiveness specifies that the insertion manipulation alters the pixel values of the host image inevitably. The signature (Cano, et al., 2002; Wu, 2002) can be a hash value of image contents or extracted characteristics. Although it is one type of non-invasive technique, the attached signature requires an additional storage in Certification Authority (CA). Besides, the signature techniques only can judge whether an image has been changed or not but cannot locate the tampered regions. Blind/passive forensic techniques (Farid, 2009; Fridrich, 2009; Lukas, Fridrich, & Goljan, 2006; Popescu & Farid, 2005; Wang, Dong, & Tan, 2009) enable detecting traces of digital forgeries in the complete absence of any form of pre-embedding or pre-registered information. Although the inactive and non-invasive image forensic methods appear in bursts and attract more attention, digital watermarking is still an immediate and mature authentication approach.

In this chapter, we attempt to survey and summarize the self-embedding watermarking which is first proposed in Fridrich and Goljan (1999). For completeness, we quote the definition of watermarking from Cox et al. (2008). Watermarking is defined as the practice of imperceptibly altering an image to embed a message about that image. Hereinafter, we give the generic classification of watermarking for drawing forth the concept of self-embedding watermarking.

According to different missions and considerations, various watermarking schemes have been proposed. Conventional invisible watermark techniques can be classified into robust watermarking, fragile watermarking and semi-fragile watermarking on the basis of the functionality. Robust watermarking (Barni, et al., 1998; Nikolaidis & Pitas, 1998; Tang & Hang, 2003), as the name suggests, possesses the ability to resist against malicious attacks and is used to declare the ownership of the image. Fragile watermarking (Barreto, et al., 2002; Li, 2004), on the other hand, is destroyed by any manipulations of pixels thus being able to locate the altered areas. However, due to the extreme sensibility, it cannot distinguish between malicious attacks and innocent manipulations such as compression, sharpening, or contrast adjustment. To address this problem, semi-fragile watermarking (Lin & Chang, 2000; Maeno, et al., 2006) is designed. It is capable of authenticating an image even after undergoing some legitimate manipulations mentioned above. In general, hash value, owner’s logo or serial number etc. serves as digital watermark for multifarious intentions. Although watermarks may survive some malicious attacks, alterations introduced in the host image is
Related Content

Successful Computer Forensics Analysis on the Cyber Attack Botnet
www.igi-global.com/chapter/successful-computer-forensics-analysis-on-the-cyber-attack-botnet/201615?camid=4v1a

Reversible Information Hiding and Its Application to Image Authentication
Masaaki Fujiyoshi and Hitoshi Kiya (2013). Multimedia Information Hiding Technologies and Methodologies for Controlling Data (pp. 238-257).
www.igi-global.com/chapter/reversible-information-hiding-its-application/70291?camid=4v1a

Creating Time-Limited Attributes for Time-Limited Services in Cloud Computing
www.igi-global.com/article/creating-time-limited-attributes-for-time-limited-services-in-cloud-computing/165106?camid=4v1a

A Subspace-Based Analysis Method for Anomaly Detection in Large and High-Dimensional Network Connection Data Streams
www.igi-global.com/chapter/subspace-based-analysis-method-anomaly/60440?camid=4v1a