A Blind Image Watermarking Scheme Utilizing BTC Bitplanes

Chun-Ning Yang, Zhejiang University, China
Zhe-Ming Lu, Zhejiang University, China

ABSTRACT

This paper presents a novel image watermarking scheme utilizing Block Truncation Coding (BTC). This scheme uses BTC to guide the watermark embedding and extraction processes. During the embedding process, the original cover image is first partitioned into non-overlapping $4 \times 4$ blocks. Then, BTC is performed on each block to obtain its BTC bitplane, and the number of ‘1’s in the bitplane is counted. If the watermark bit to be embedded is ‘1’ and the number of ‘1’s is odd, or the watermark bit to be embedded is ‘0’ and the number of ‘1’s is even, then no change is made. Otherwise, by changing at most three pixels in the original image block, the number of ‘1’s (or ‘0’s) in the renewed bitplane are forced to be odd for the watermark bit ‘1’ or to be even for the watermark bit ‘0’. During the extraction process, BTC is first performed on each block to obtain its bitplane. If the number of ‘1’s in the bitplane is odd, then the embedded watermark bit is ‘1’. Otherwise, the embedded watermark bit is ‘0’. The experimental results show that the proposed watermarking method is semi-fragile except for the changes in brightness and contrast; therefore, the proposed method can be used for image authentication.

Keywords: Blind Watermarking, Block Truncation Coding, Content Authentication, Fragile Image Watermarking, Information Hiding

INTRODUCTION

In the digital information network age, many media formats are easy to copy using a machine, allowing consumers to distribute copies via the Internet to their friends. On the other hand, digital media can be easily edited and modified by various multimedia tools. As a result, copy protection, digital rights management and content authentication have become three urgent and serious issues in the digital world. Copy protection refers to the technology attempting to frustrate copying, and not to make the legal remedies available to users whose copyrights are violated. Digital rights management (DRM) stands for the access control technology used by hardware manufacturers, publishers, copyright holders and individuals to inhibit uses of digital content that is not desired or intended by the content provider. Unlike data authentication techniques that check whether the data have been changed or not, content authentication refers to the technique used to verify whether the content or semantics of the media has been changed or not. Over the last two decades, digital watermarking has provided an effective solution to above problems. Digital watermarking de-
cribes the technologies to embed information, for example a number or a text or an image, into the digital media, such as images (Niu et al., 2000a, 2000b; Luo et al., 2011), video (Wang et al., 2005; Wang, Lu, Li, & Sun, 2009; Wang, Lu, Liang, & Zheng, 2009; Wu et al., 2011) and audio (Lu et al., 2005b; Yan et al., 2006), in order to protect the copyright or authenticate the content.

Digital watermarking methods can be categorized from different points of view. First, from the application point of view, most digital watermarking methods can be broadly classified into three categories: robust, fragile and multipurpose schemes. Robust watermarking schemes (Lu & Sun 2000; Lu et al., 2000, 2002; Niu et al., 2000a, 2000b; Wang et al., 2005; Wang, Lu, Liang, & Zheng, 2009; Wu et al., 2011) are mainly designed for copyright protection where the watermark is still detectable after various removal procedures (accidental or malicious) called attacks. On the other hand, fragile watermarking methods (Lu et al., 2003, 2005b; Luo et al., 2011; Yang & Lu, 2011) are basically designed for integrity check and content authentication where the slightest alteration of the image is detectable or noticeable in the content of the watermark. In addition, recently several multipurpose watermarking schemes (Lu et al., 2005a, 2007; Wang, Lu, Li, & Sun, 2009) have been presented to simultaneously fulfill multiple purposes such as copyright protection, content authentication and multimedia retrieval. Second, from the visibility point of view, there are two types of digital watermarks addressed in the existing literature, visible and invisible watermarks. A visible watermark (Luo et al., 2007) typically contains a visible message or a company logo indicating the ownership of the image. On the other hand, the invisibly watermarked digital content appears visually very similar to the original. Most watermarking schemes are invisible. Third, from the embedding domain point of view, watermarking schemes can be performed in the spatial domain, transform domains (e.g., DCT, DWT, DFT) or compressed domains (e.g., JPEG, JPEG2000, VQ, BTC). The spatial domain schemes directly modify the multimedia data to hide information. Their advantage is the low computation complexity. However, they are not robust enough to resist various attacks. Transform domain-based techniques (Niu et al., 2000a, 2000b; Luo et al., 2011; Wang et al., 2005, Wang, Lu, Li, & Sun, 2009; Wang, Lu, Liang, & Zheng, 2009) have been found to offer several advantages over spatial domain-based methods, in terms of perceptibility and robustness. Several transforms, such as DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform) and HT (Hadamard transform), are mainly used to hide watermarks in the coefficients of transform matrices. Some other transforms such as discrete fractional random transform (Luo et al., 2011) have been applied in image watermarking. Recently, since most of images are stored in compressed formats such as JPEG and JPEG2000 or transmitted based on VQ and BTC, many scholars have been engaged in the compressed-domain watermarking schemes. Among them, VQ-based and BTC-based methods are attractive for they are two famous block-based image compression techniques with easy implementation and high efficiency. In the past ten years, several vector quantization (VQ) based watermarking schemes (Lu et al., 2000, 2003, 2005a; Lu & Sun, 2000) have been proposed as a special branch, where the watermark information is embedded in codeword indices. These algorithms can be classified into three categories: robust, semi-fragile and multipurpose schemes. The algorithms proposed in Lu et al. (2000) and Lu and Sun (2000) are robust, the algorithm proposed in Lu et al. (2003) is semi-fragile, and the algorithm proposed in Lu et al. (2005a) is a multipurpose scheme for both copyright protection and content authentication.

Besides VQ, block truncation coding (BTC) (Mitchell & Delp, 1979) is another efficient block-based lossy image compression technique. It uses a quantizer to reduce the number of grey levels in each block whilst maintaining the same mean and standard deviation. Another variation of BTC is absolute moment
A Novel Progressive Secret Image Sharing Scheme Based on Arithmetic Mean
www.igi-global.com/article/a-novel-progressive-secret-image-sharing-scheme-based-on-arithmetic-mean/182462?camid=4v1a