Robust Reversible Data Hiding Scheme Based on Gravity Center Difference

Qunting Yang, College of Air Traffic Management, Civil Aviation University of China, Tianjin, China

Tiegang Gao, College of Software, Nankai University, Tianjin, China

ABSTRACT

This paper presents a robust reversible data hiding scheme in wavelet domain. The proposed scheme divides the permuted image into non-overlapping blocks and then gets sub-blocks. The generated sub-blocks are transformed by discrete wavelet transform and the corresponding low frequency regions are gotten, respectively. The gravity centers of low frequency regions in every non-overlapping block are very similar. These gravity center pairs are utilized to embed secret data since the insensitivity of the gravity centers to malicious tampering. Experimental results show that the original image can be recovered without any distortion after the hidden data have been extracted if the stego image has not been altered. Meanwhile hidden data can still be extracted without error when the image is compressed by JPEG and JPEG2000 to a certain extent. Compared with some existing literatures, the security, payload and robustness of the proposed scheme are significantly improved.

Keywords: Data Hiding, Gravity Center Difference, Robust, Reversible, Security

INTRODUCTION

As an important way to protect secret information, data hiding technique has been extensively studied recently. Data hiding is different from classical encryption, which hides secret information into a cover object (e.g., image, video, audio, text) to create a stego medium with little distortion (Provos & Honeyman, 2003; Li et al., 2010). In general, data hiding includes digital watermarking and steganography(Petitcolas et al.,1999) .Digital watermarking is used for copyright protection (Nikolaidis & Pitas, 1998; Lin et al., 2001), authentication (Lin & Chang, 2001; Lu &
Liao, 2001), and transaction tracking (wong et al., 2005), etc., whereas steganography undetectably alters a cover object to conceal a secret message (Cox et al., 2007). Usually, three different aspects in steganographic systems contend with each other: payload, imperceptibility, and robustness (Langelaar et al., 2000; Sabeti et al., 2010). The tradeoffs of these aspects vary with the application domains and users’ requirements.

Many steganographic techniques about embedding data into images have been proposed. For example, Wu and Tsai (2003) introduced a steganography based on pixel-value differencing, which hided large amount of secret bits into an image by modifying the difference values between pairs of adjacent pixels. To enhance the security, Zhang and Wang (2004) proposed a modified scheme by selecting the length of the intervals randomly. Chen et al. (2010) proposed a steganography mechanism using hybrid edge detector. Hsiao and Chang (2011) proposed an adaptive steganographic method based on the measurement of just noticeable distortion profile measurement.

In general, embedding secret data into a cover image often leads to the degradation of embedded image and the original image can’t be recovered. However, in some applications, such as military image systems, medical diagnosis, and art works, it is critical for an original image to be recovered or reversed after the hidden data are extracted. This technique, which is called distortion-free or lossless data hiding, has drawn tremendous attention in recent years. Tian (2003) proposed a reversible data embedding scheme with high payload and good imperceptibility and then Alattar (2004) generalized Tian’s scheme. Kim et al. (2008) introduced histogram based reversible data hiding technique by using subsampling, and some other reversible image steganographic schemes, such as (Lee et al., 2008; Kieu & Chang, 2009; Wu et al., 2010; Chang & Kieu, 2010), are also introduced recently.

The stego images may be confronted with some incidental modifications in the transmission, such as image compression and sometimes unavoidable addition of random noise, which are below a certain level that can change the content of an image. The data hiding schemes mentioned above are all fragile schemes. The hidden data cannot be recovered correctly after compression or other incidental modification. To extract the hiding data correctly when stego image goes through unmalicious alteration, data hiding scheme with good robustness, also known as semi-fragile data hiding scheme, is introduced. Robust data hiding scheme may be more practical than fragile scheme in many applications since it allows some incidental modification, such as image compression and noise addition. In relative literatures, De Vleeschouwer et al. (2003) presented a robust reversible data hiding technique employing a circular interpretation of bijective transformations together with modulo-256 addition to allow secret data to be appended. Then Solanki et al. (2004) proposed a robust image-adaptive data hiding scheme based on information theoretic analyses to hide large volumes of data with low perceptual degradation. Zou et al. (2006) introduced a robust lossless data hiding scheme that classified a block into one of four special categories to prevent overflow/underflow and hence didn’t suffer from annoying salt-and-pepper noise. Ni et al. (2008) proposed a robust lossless image data hiding scheme designed for semi-fragile image authentication based on patchwork theory. Then based on Ni’s scheme, Zeng et al. (2010) realized a similar robust lossless data hiding algorithm by introducing two thresholds. Lin et al. (2009) proposed a data hiding scheme which could tolerate a little distortion in spatial domain. Gao et al. (2009) presented a reversible robust data hiding scheme focused on the reversibility of reversible schemes. All these robust algorithms utilized the distribution characteristics of the histogram to achieve robust lossless data hiding. In these schemes, the hidden data can be extracted correctly and cover image can be losslessly recovered. In the meantime, the hidden data could still be extracted correctly when stego image goes through incidental modification to a certain extent.
Related Content

A Framework for Dark Web Threat Intelligence Analysis
www.igi-global.com/article/a-framework-for-dark-web-threat-intelligence-analysis/210140?camid=4v1a

Identity Theft Through the Web
www.igi-global.com/chapter/identity-theft-through-web/60940?camid=4v1a

Female and Male Hacker Conferences Attendees: Their Autism-Spectrum Quotient (AQ) Scores and Self-Reported Adulthood Experiences
Bernadette H. Schell and June Melnychuk (2011). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 144-169).
www.igi-global.com/chapter/female-male-hacker-conferences-attendees/46424?camid=4v1a