Expert Systems with Applications 42 (2015) 8184–8197

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Significant region based robust watermarking scheme in lifting wavelet transform domain

Vivek Singh Verma [a], Rajib Kumar Jha [b,*], Aparajita Ojha [a]

[a] PDPM, Indian Institute of Information Technology, Design and Manufacturing Jabalpur, 482005, India
[b] Indian Institute of Technology Patna, Bihar 800013, India

ARTICLE INFO

Article history:
Available online 6 July 2015

Keywords:
Blind watermarking
Lifting wavelet transform
Block selection procedure
Significant region

ABSTRACT

With the aim of designing a more robust digital watermarking scheme against various unintentional and intentional attacks, a significant region (SR) based image watermarking technique is proposed in the present paper using lifting wavelet transform (LWT). While the energy compaction property of LWT provides higher tolerance against image distortion as opposed to conventional wavelet transform, the proposed block selection procedure provides greater security over the existing watermarking approaches. Non-overlapping coefficient blocks from the lowpass subband are selected after applying three levels of LWT and using certain criterion based on minimum coefficient difference and a threshold value. To disguise the intruder completely, secret key based randomization of coefficients, blocks, and watermark bits is incorporated. Maximum coefficients difference of each selected block and the same threshold value are then used for deciding which block to choose for embedding the bit 0 or 1. Performance of the proposed method is analyzed and compared with some of the existing schemes that demonstrates that the proposed scheme not only outperforms other methods with respect to various attacks for most of the cases, but also maintains a satisfactory image quality.

1. Introduction

In recent years, digital watermarking has enlisted considerable prominence within the research community due to its remarkable benefits over the traditional data hiding techniques, especially copyright protection or authentication based applications. In case of copyright protection based applications, watermarking system still face the challenge of being robust against contaminated environment, which consist of a series of lawful/lawless deformations. These deformations are slightly comprehensible based on application environment and the level of access the attacker has. Customarily, a trade-off between watermark imperceptibility, robustness and security is selected depending on the application. Broadly, watermarking techniques are developed either in the spatial domain or in the transform domain. A review of the literature reveals that transform domain techniques are more robust to various signal processing attacks as compared with spatial domain techniques. Various spatial domain based techniques have been proposed with focus on ensuring the integrity of digital media and other related issues (see for example, Nikolaidis & Pitas (1998), Luo, Chen, Chen, Zeng, & Xiong (2010, 2011), Wang, Chang, Nguyen, & Li (2013) and Li, Li, Li, & Yang (2013)). More recently, a reversible data hiding scheme with focus on high-fidelity of digital images was proposed by Li et al. (2013). A new prediction strategy called pixel-value-ordering (PVO) and the well-known prediction-error expansion (PEE) technique is used for data embedding. The incorporation of PVO into PEE has an advantage in reducing the number of shifted pixels, and thus it can alleviate the degradation in image quality.

Numerous watermarking methods have also been proposed using transform domain and most of these methods analyze watermark perceptibility against various signal processing attacks (see for example, Cox, Kilian, Leighton, & Shamoon (1997), Barni, Bartolini, Cappellini, & Piva (1998), Kundur & Hatzinakos (1998), Chen, Ouhyoung, & Wu (2000), Hsieh, Tseng, & Huang (2001), Wang & Lin (2004), Lin, Wang, & Horng (2009), Run et al. (2011), Wang, Lin, & Yang (2011), Fu (2013), Das, Panigrahi, Sharma, & Mahapatra (2014), Ali & Ahn (2014), Mishra, Agarwal, Sharma, & Bedi (2014) and Ali, Ahn, Pant, & Siarry (2015)). Recently, Lin et al. (2009) proposed a wavelet-tree-based watermarking method using distance vector of a binary cluster for copyright protection. In this method, wavelet trees are classified into two clusters using the distance vector to denote binary watermark bits. The two minimum wavelet coefficients in a wavelet tree are used to reduce

* Corresponding author.
E-mail addresses: viveksv10@gmail.com (V.S. Verma), jharajib@gmail.com (R.K. Jha), aparajitaojha@gmail.com (A. Ojha).

http://dx.doi.org/10.1016/j.eswa.2015.06.041
0957-4174/

distortion of a watermarked image, and the watermark bits are embedded by quantizing the two smallest coefficients of a wavelet tree. In case of watermark extraction, an adaptive thresholding based approach is adopted. Another version of wavelet tree based watermarking scheme is proposed by Run et al. (2011). In this scheme, the watermark bits are embedded by quantizing the two maximum coefficients of a wavelet tree. An adaptive thresholding based approach is applied for watermark extraction. Though, both the techniques (Lin et al., 2009; Run et al., 2011) show more robustness against various signal processing operations, but fail to resist JPEG compression with high compression ratio efficiently. We have also analyzed that in the experimental section of both the techniques (Lin et al., 2009; Run et al., 2011). Tables 1–3 appear to be seriously flawed. One can observe that after applying different signal processing operations to the watermarked image, the extracted watermarks are exactly similar to its original version. For example, in Lin et al. (2009), the normalized correlation coefficient (NC) values in case of JPEG compression with quality factors 10 and 100 are 0.24 and 1.0, respectively. Though, the NC value indicates the degradation (at JPEG (10)) in watermark extraction but the extracted watermark in both cases are perceptually similar which is not possible. Therefore, the statement given in experimental section of Lin et al. (2009) "The smaller the quality factor is, the more unclear the extracted watermark will be" indicates contradiction with results in terms of extracted watermark of Table 1 in Lin et al. (2009). Similarly, in Run et al. (2011), the NC values in case of JPEG compression with quality factors 10 and 100 are 0.32 and 1.0, respectively. Hence, the statement given in experimental section of Run et al. (2011) "The less the quality factor is, the vague the extracted watermark is" indicates contradiction with results in terms of extracted watermark of Table 1 in Run et al. (2011). Also, in all other attack cases, no distortions in extracted watermarks are shown in Tables 2 and 3 of both the techniques (Lin et al., 2009; Run et al., 2011).

Adapting discrete wavelet transform (DWT) and genetic algorithm (GA) Ramanjaneyulu and Rajarajeswari (2012) have recently proposed a new strategy for copyright protection. In this scheme, watermark embedding and extraction processes are characterized with quantitative parameters of watermarked image and GA is used for parameter optimization. The method exhibits robustness against various image processing operations, but fails to achieve sufficient robustness against JPEG compression and sharpening operation. Using Bose–Chaudhuri–Hocquenghem (BCH) code, Fu (2013) proposed a novel discrete cosine transform (DCT) based image watermarking scheme. The watermark bits are embedded into the host by modulating the relationships between the selected DCT coefficients. However, the proposed method does not handle JPEG compression efficiently. More recently, Ali et al. (2015) presented a robust image watermarking scheme in the wavelet domain based on singular value decomposition (SVD) and artificial bee colony (ABC). In this approach, ABC is employed to obtain the optimized threshold and compensation parameters. The method exhibits robustness against various signal processing operations, but it is less efficient in case of median filtering, scaling, and salt and pepper noise attacks.

Table 1
Results of test image "Lena" under different attacks.

Attacks	NC	BER	Extracted watermark
Md (3 × 3)	0.9570	0.0215	
Md (5 × 5)	0.8125	0.0938	
Avg (3 × 3)	0.8945	0.0527	
Avg (5 × 5)	0.7383	0.1309	
GF	0.9766	0.0117	
Shp	0.9766	0.0117	
HE	0.9297	0.0352	
Gs (0.01)	0.9727	0.0137	
Gs (0.02)	0.8555	0.0723	
Slp (0.01)	0.7539	0.1230	
Spn (0.01)	0.7461	0.1270	
Ap1.5	0.8633	0.0684	
Ap1.8	0.6133	0.1934	
Scl (1/2)	0.9844	0.0078	
Cr (1/4)	0.9336	0.0332	
Rt(0.1^0)	0.8594	0.0703	

Utilizing several benefits of LWT over conventional wavelet transform, various LWT based watermarking techniques are developed over the last few years (see for example, Phadikar, Maity, & Kundu (2008), Bohra, Farooq, & Izharuddin (2009), Jinna & Ganesan (2010), Wang, Li, Yang, & Guo (2010), Lei, Soon, Zhou, Li, & Lei (2012), Gu & Gao (2013), Verma & Jha (2014) and Makbol & Khoo (2014)). Phadikar et al. (2008) proposed a dither modulation (DM) based data hiding scheme using DWT via lifting for quality access control of images. Lei et al. (2012) proposed an audio watermarking technique based on LWT, SVD, and Quantization Index Modulation (QIM) with synchronization code technique to withstand desynchronization attack. Another interesting reversible watermarking technique using chaotic systems has been proposed by Gu and Gao (2013) that uses protection for important digital media, such as medical and military images. This scheme claims to achieve larger threshold space of reversibility and robustness against image compression. However, with the increase in the threshold value for maintaining robustness, reversibility is compromised. So, one needs to maintain a balance between reversibility and robustness. More recently, a combined LWT-SVD based robust and secure digital image watermarking scheme is presented by Makbol and Khoo (2014). Although, the scheme produces good resistance against a large number of geometric and non-geometric operations, for higher compression ratios, performance of the schemes deteriorates against JPEG compression, although marginally.

In essence, most of the existing schemes demonstrate robustness against some categories of attacks but fail to perform well against other types of attacks. A review of literature suggests that the challenge remains in the field of digital watermarking in designing schemes that are more robust against a broad range of attacks and maintain reasonable image quality. Most of the schemes underperform especially when image distortion or compression is high. With the aim to provide higher security and robustness, a digital watermarking scheme is proposed in the present paper that not only outperforms other methods with respect to various attacks for most of the cases, but also maintains a satisfactory image quality.

1.1. Key contribution

The proposed work is inspired by the techniques developed by Li et al. (2013), Lin et al. (2009) and Wang et al. (2011) with focus on robustness and security. The concept of selecting regions for watermark embedding is based on Li's method (Li et al., 2013). The difference between Li's method (Li et al., 2013) and the proposed work is that in Li's method, regions for watermark embedding are defined on the basis of pixel error (PE), while, in proposed scheme the regions are selected on the basis of minimum coefficient difference of LH3 subband. And, the difference between Lin's method (Lin et al., 2009) and the proposed scheme is that in Lin's method, watermark is embedded by quantizing the minimum coefficients of lower frequency subband of wavelet tree, while in the proposed scheme, watermark is embedded by quantizing the maximum coefficients of lower frequency subband of LWT. Hence, in the proposed scheme a different methodology for watermark insertion and its extraction is incorporated.