Journal of King Saud University – Computer and Information Sciences (2015) **27**, 393–401

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network

Yahya AL-Nabhani, Hamid A. Jalab *, Ainuddin Wahid, Rafidah Md Noor

Faculty of Computer Science and Information Technology, University Malaya, 50603 Kuala Lumpur, Malaysia

Received 26 October 2014; revised 17 February 2015; accepted 25 February 2015
Available online 10 September 2015

KEYWORDS

Watermarking;
Discrete wavelet;
Probabilistic neural networks

Abstract Digital watermarking, which has been proven effective for protecting digital data, has recently gained considerable research interest. This study aims to develop an enhanced technique for producing watermarked images with high invisibility. During extraction, watermarks can be successfully extracted without the need for the original image. We have developed discrete wavelet transform with a Haar filter to embed a binary watermark image in selected coefficient blocks. A probabilistic neural network is used to extract the watermark image. To evaluate the efficiency of the algorithm and the quality of the extracted watermark images, we used widely known image quality function measurements, such as peak signal-to-noise ratio (PSNR) and normalized cross correlation (NCC). Results indicate the excellent invisibility of the extracted watermark image (PSNR = 68.27 dB), as well as exceptional watermark extraction (NCC = 0.9779). Experimental results reveal that the proposed watermarking algorithm yields watermarked images with superior imperceptibility and robustness to common attacks, such as JPEG compression, rotation, Gaussian noise, cropping, and median filter.

1. Introduction

Digitization is occurring worldwide, which can be attributed to the rapid progress and advancement in information technology. This phenomenon exhibits both advantages and disadvantages. The problem regarding the ownership of digital media often draws interest from researchers. Digital information may be copied, attacked, or altered during storage or transmission. Thus, effective watermarking methods that protect digital data need to be developed. Moreover, information should be shared to obtain optimal benefits and utilization.

* Corresponding author.
E-mail addresses: yahyanabhani@yahoo.com (Y. AL-Nabhani), hamidjalab@um.edu.my (H.A. Jalab), ainuddin@um.edu.my (A. Wahid), fidah@um.edu.my (R.M. Noor).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2015.02.002

Thus, the security and confidentiality of such information should be seriously addressed.

A digital medium can refer to any kind of digital data, such as text, image, video, or audio. Digital watermarking protects digital media and verifies its legitimate owner. Watermarking was developed from steganography. Both techniques use the concept of embedding information into cover data media (Ghaleb Al-Jbara et al., 2012).

A watermarking scheme should, at the very least, possess the following qualities: perceptually invisible (or transparent), difficult to remove without seriously affecting image quality, and resistant to image processing attacks. Watermarks can be classified into two main types: visible and invisible. Visible watermarks, such as those used in company logos, are perceptible, whereas invisible watermarks are imperceptible and embedded on unknown areas in the host data. In addition, watermarks can be categorized into two classes according to the processing domain: spatial domain and transform or frequency domain. The former embeds the watermark by directly modifying the pixel values of the original image. Simplicity and ease of implementation are the two advantages provided by spatial domain algorithms over other similar watermarking algorithms (Zheng et al., 2007). Spatial domain algorithms are less robust than other types of watermarking algorithms because they are more vulnerable to compression, filtering, or noise attacks (Zheng et al., 2007; Lai and Tsai, 2010). Transform domain methods, such as discrete cosine transform, discrete Fourier transform, and discrete wavelet transform (DWT), embed the watermark by modulating the coefficients of the original image in a transform domain (Huang et al., 2008; Seng et al., 2011, 2009). The transform domain method is more robust than the spatial domain method against compression, filtering, rotation, cropping, and noise attacks (Lu, 2005). The wavelet domain, which is a category of the transform domain, is considered an efficient watermark-embedding domain. Embedding an excessive amount of data in the frequency domain can significantly degrade the quality of the watermarked image and result in imperceptibility constraints (Wang, 2011). In addition, watermarking in the DWT domain has drawn considerable attention because of its desirable time-frequency features and accurate matching of the human visual system (Kashyap and Sinha, 2012).

Artificial intelligence contributes to the further development of watermarking techniques. Artificial neural networks enhance the performance of conventional watermarking methods by memorizing the relation between the watermark and the corresponding watermarked image.

Several studies (Huang et al., 2008; Chen and Chen, 2010; Ramamurthy and Varadarajan, 2012; Mei et al., 2002) presented a blind image watermarking scheme that embeds watermark messages into different wavelet blocks according to back-propagation neural networks. Zhang (2009) proposed a blind watermark with the use of the radial basis neural network in the wavelet domain. The watermark can be precisely recovered from the watermarked image without the original and "watermark images."

Efforts have recently been directed toward the use of probabilistic neural network (PNN) in the wavelet domain. A blind watermarking scheme based on PNNs in the wavelet domain was proposed in Wen et al. (2009). The statistical properties of the dual-tree wavelet transform were used to embed the watermark bits into edges and textures to achieve watermark safety and imperceptibility. However, the watermark-embedding algorithm depends only on the standard deviations of each coefficient block of the dual-tree complex wavelet transform. Thus, the quality of the watermarked image is degraded after embedding. To our knowledge, this study is thus far the only published work that is based on PNNs in the wavelet domain.

In this work, we propose an imperceptible and robust blind watermarking algorithm based on the PNN in the wavelet domain. The proposed algorithm focuses on maintaining the invisibility and quality of the watermarked image by selecting the best embedding positions in the block-based wavelet coefficient. PNN is then applied to memorize the relation between the watermark and the corresponding watermarked image. Thus, the watermark can be recovered from the watermarked image without the original and watermark images. Experimental results demonstrate that the proposed method performs efficiently in terms of peak signal-to-noise ratio (PSNR) and normalized cross correlation (NCC), as well as exhibits high robustness to various common attacks, such as JPEG compression, rotation, Gaussian noise, cropping, and median filter. These experimental results are finally compared with the results of previous studies.

The remainder of this paper is organized as follows: Section 2 describes the proposed algorithm. Section 3 presents the experimental results. Section 4 concludes the paper.

2. Proposed watermarking algorithm

The proposed algorithm includes three steps: decomposing the cover image, embedding, and extraction. A binary watermark image will be used as the watermark for embedding. The trained PNN is used to extract the watermark during watermark recovery.

2.1. Watermark-embedding algorithm

The watermark-embedding method is shown in Fig. 1. This algorithm essentially includes the following steps: wavelet decomposition, block splitting, watermark embedding, wavelet reconstruction, and watermarked image testing.

In the algorithm process, three levels of wavelet decomposition are performed for the original cover image with the use of the Haar filter wavelet. The Haar wavelet is well known for its simplicity and speed of computation (Zheng et al., 2007; Zhang, 2009). In the DWT, the signal passes through two complementary filters and emerges as two signals: approximation and details. This process is called decomposition or analysis. The components can be assembled back into the original signal without loss of information. This process is called reconstruction or synthesis (Zhang, 2009; MathWorks). For image watermarking, the fundamental idea behind the use of wavelets is to conduct an analysis according to scale and time. According to Lin et al. (2009), the DWT approach is the easiest and most efficient technique for image watermarking. However, the most important aspect of DWT embedding is the selection of the DWT coefficients to be used for embedding and the location in which to embed the watermark within the selected coefficients.

In this study, three levels of 2D-Haar DWT decomposition are used for the original cover image. Haar wavelet uses two