Computers and Electrical Engineering 37 (2011) 695–713

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Geometrically invariant image watermarking using SVR correction in NSCT domain ☆

Yang Hong-ying [a], Wang Xiang-yang [a,b,c,*], Chen Li-li [a]

[a] School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, China
[b] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China
[c] Network and Data Security Key Laboratory of Sichuan Province, Chengdu 611731, China

ARTICLE INFO

Article history:
Available online 6 August 2011

ABSTRACT

Based on the support vector regression (SVR) geometric distortions correction, we propose a robust image watermarking algorithm in nonsubsampled contourlet transform (NSCT) domain with good visual quality and reasonable resistance toward geometric attacks in this paper. Firstly, the NSCT is performed on original host image, and corresponding low-pass subband is selected for embedding watermark. Then, the selected low-pass subband is divided into small blocks. Finally, the digital watermark is embedded into host image by modulating the NSCT coefficients in small blocks. In digital watermark detecting procedure, the SVR geometrical distortions correction is utilized. Experimental results show that the proposed image watermarking is invisible, and robust against common image processing and some geometrical attacks.

1. Introduction

With the rapid growth and widespread use of network distributions of digital media content, there is an urgent need for protecting the copyright of digital content against piracy and malicious manipulation. Digital watermarking has been proposed as a possible and efficient answer to these concerns. While the most prominent application of watermarking is copyright protection, others including fingerprinting, broadcast monitoring, digital media authentication, and copy protection are important research areas [1]. For different purposes, digital watermarking has been branched into two classifications: robust watermarking technique and fragile watermarking technique. Robust digital watermarking is used to protect ownership of the digital media. In contrast, the purpose of fragile watermarking technique is digital media authentication, that is, to ensure the integrity of the digital media.

In recent years, there is an unprecedented development in the robust image watermarking field. On the other hand, attacks against image watermarking systems have become more sophisticated [2]. In general, these attacks on watermarking systems can be categorized into noise-like common image processing operations and geometric attacks. While the noise-like common image processing operations, such as lossy compression, noise addition, and lowpass filtering, reduces watermark energy, geometric attacks can reduce synchronization errors between the extracted watermark and the original watermark during the detection, even though the watermark still exists in the watermarked image. Nowadays, several approaches that counterattack geometric attacks have been developed. These schemes can be roughly divided into invariant transform, template insertion, and feature-based algorithms [3–5].

☆ Reviews processed and approved for publication to Dr. Ferat Sahin.

* Corresponding author at: School of Computer and Information Technology, Liaoning Normal University, Dalian 116029, China. Tel.: +86 0411 85992415; fax: +86 0411 85992323.
E-mail address: wxy37@126.com (X.-y. Wang).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.07.002

Invarianttransform: The most obvious way to achieve resilience against geometric attacks is to use an invariant transform. In [6–8], the watermark is embedded in an affine-invariant domain by using Fourier–Mellin transform, generalized Radon transform, geometric moments, and histogram shape, respectively. Despite that they are robust against global affine transformations, those techniques involving invariant domain suffer from implementation issues and are vulnerable to mixed attacks.

Template insertion: Another solution to cope with geometric attacks is to identify the transformation by retrieving artificially embedded references. By focusing on a simple example, Barni [9] investigated the effectiveness of exhaustive watermark detection and resynchronization through template matching against geometric attacks. Liu et al. [10] presents an image rectification scheme that can be used by any image watermarking algorithm to provide robustness against rotation, scaling, and translation (RST). In the watermarking, a small block is cut from the log-polar mapping (LPM) domain as a matching template, and a new filtering method is proposed to compute the cross-correlation between this template and the magnitude of the LPM of the image having undergone RST transformations to detect the rotation and scaling parameters. However, this kind of approach can be tampered with by the malicious attack.

Feature-based: The last category is based on media features. Its basic idea is that, by binding the watermark with the geometrically invariant image features (local feature region, LFR), the watermark detection can be done without synchronization error. Lee et al. [11] propose a geometrically invariant watermarking method that uses circular Hough transform for watermark synchronization. Through circular Hough transform, the circular features are extracted that are invariant to geometric attacks. Seo et al. [12] introduce a content-based image watermarking algorithm based on scale-space representation. Mayank et al. [13] presented a 3-level RDWT biometric watermarking algorithm to embed the voice biometric MFC coefficients in a color face image of the same individual for increased robustness, security and accuracy. Based on Harris–Laplace detector and scale-space theory, Wang et al. [14] propose a feature-based digital image watermarking scheme in DFT domain. In [15], Li et al. present a novel robust image watermarking scheme for resisting geometric attacks. Watermark synchronization is first achieved by local invariant regions which can be generated using scale normalization and image feature points. The watermark is embedded into all the local regions repeatedly in spatial domain. Deng et al. [16] give a content-based watermarking scheme that combines the invariant feature extraction with watermark embedding by using moments. Pham et al. [17] present a robust object-based watermarking algorithm using the local image feature in conjunction with a data embedding method based on DCT, and the digital watermark is embedded in the DCT domain of randomly generated blocks in the selected object region. It is not difficult to see that the feature-based approaches are better than others in terms of robustness. However, some drawbacks indwelled in current feature-based schemes restrict the performance of watermarking system. First, the feature point extraction is sensitive to image modification. Second, the computational complexity in calculating the features of an image before watermark detection is added. Third, the volume of watermark data is lesser.

In order to effectively resolve the problem of resisting geometric attacks, the support vector machine (SVM) theory is introduced to the image watermarking domain. Fu et al. [18] first embed template and watermark into original image in the same way, then a SVM train model is obtained by using the template samples, and the output of SVM model is obtained and the watermark is extracted. In scheme [19,20], in order to obtain the rotation, scaling and translation (RST) parameters, the SVM are utilized to learn image geometric pattern represented by six combined low order image moments. The watermark extraction is carried out after watermarked image has been synchronized without original image. Wang et al. [21] proposed a robust image watermarking detection algorithm against geometric attacks, in which the steady pseudo-Zernike moments and Krawtchouk moments are utilized. Tsai et al. [22] propose a novel watermarking technique called SVM-based color image watermarking (SCIW) for the authentication of color images. The SCIW method utilizes the set of training patterns to train the SVM and then applies the trained SVM to classify a set of testing patterns. Following the results produced by the classifier, the SCIW method retrieves the hidden watermark without the original image during watermark extraction. Li et al. [23] introduce a novel semi-fragile watermarking scheme based on SVM. This scheme first gives a definition of wavelet coefficient direction tree, then the relation model between the root node and its offspring nodes is established using SVM, and further watermark is embedded and extracted based on this relation model.

Based on a large number of theory analyses and experimental results, we can easily come to the conclusion that it is possible to resist geometric attacks by utilizing the advanced SVM, but the current SVM based image watermarking have shortcomings as follows: they are not very robust against some tacks, such as edge sharpening, histogram equilibrium, length-width ratio change, cropping, mixed attacks, etc. In digital watermark detection procedure, the original watermark signal is usually needed, so it is unfavorable to practical application.

In this paper, we propose a geometrically invariant image watermarking scheme by using SVR correction in NSCT domain. Firstly, the NSCT is performed on original host image, and corresponding low-pass subband is selected for embedding watermark. Then, the selected low-pass subband is divided into small blocks. Finally, the digital watermark is embedded into host image by modulating the NSCT coefficients in small blocks. The main steps of digital watermark detecting procedure include: (1) some low-order Tchebichef moments of test image are computed, which are regarded as the effective feature vectors; (2) the appropriate kernel function is selected for training, and a SVR training model can be obtained; (3) the test image is corrected with the well trained SVR Model; (4) the digital watermark is extracted from the corrected test image.

The rest of this paper is organized as follows: Section 2 presents the basic theory about NSCT. In Section 3, the SVR technique is described. Section 4 presents the effectiveness of Tchebichef moments. Section 5 contains the description of our watermark embedding procedure. Section 6 covers the details of the watermark detection procedure. Simulation results in Section 7 will show the performance of our scheme. Finally, Section 8 concludes this presentation.