Applied Soft Computing 12 (2012) 887–903

Contents lists available at SciVerse ScienceDirect

Applied Soft Computing

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

A new SVM-based image watermarking using Gaussian–Hermite moments☆

Wang Xiang-Yang[a,b,c,*], Miao E-No[a], Yang Hong-Ying[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:
Received 8 November 2010
Received in revised form 15 August 2011
Accepted 15 October 2011
Available online 4 November 2011

Keywords:
Image watermarking
Geometric attack
Support vector machine
Gaussian–Hermite moments
Nonsubsampled contourlet transform

ABSTRACT

Geometric attack is known as one of the most difficult attacks to resist, for it can desynchronize the location of the watermark and hence causes incorrect watermark detection. It is a challenging work to design a robust image watermarking scheme against geometric attacks. Based on the support vector machine (SVM) and Gaussian–Hermite moments (GHMs), 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 adaptively the NSCT coefficients in small block. The main steps of digital watermark detecting procedure include: (1) some low-order Gaussian–Hermite moments of training image are computed, which are regarded as the effective feature vectors; (2) the appropriate kernel function is selected for training, and a SVM training model can be obtained; (3) the watermarked image is corrected with the well trained SVM model; (4) the digital watermark is extracted from the corrected watermarked image. Experimental results show that the proposed image watermarking is not only invisible and robust against common image processing operations such as filtering, noise adding, JPEG compression, etc., but also robust against the geometric attacks.

1. Introduction

The advance of computer technologies and the proliferation of the Internet have made reproduction and distribution of digital information (image, audio, video, etc.) easier than ever before. Copyright protection of intellectual properties has, therefore, become an important topic. One way for copyright protection is digital watermarking, which means embedding of certain specific information about the copyright holder (company logos, ownership descriptions, etc.) into the media to be protected [1,2]. For different purposes, digital watermarking methods for images are usually categorized into two types: robust watermarking and fragile watermarking. Robust digital watermarking is used to protect ownership of the digital media. In contrast, the purpose of fragile watermarking technique is digital media authentication, i.e., 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 [3]. 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 low-pass 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 [4,5].

Invariant transform: 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. Tai et al. [9] presented a reversible data-hiding scheme based on histogram modification.

☆ This work was supported by the National Natural Science Foundation of China under Grant No. 60773031 and 60873222, the Open Foundation of State Key Laboratory of Information Security of China under Grant No. 04-06-1, the Open Foundation of Network and Data Security Key Laboratory of Sichuan Province, the Open Foundation of Key Laboratory of Modern Acoustics Nanjing University under Grant No. 08-02, and Liaoning Research Project for Institutions of Higher Education of China under Grant No. 2008351 and L2010230.

* 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).

1568-4946/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.asoc.2011.10.003

They exploit a binary tree structure to solve the problem of communicating pairs of peak points. 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 [10,11]. Liu et al. [12] 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, the watermark detection can be done without synchronization error [13–17]. Deng et al. [18] give a content-based watermarking scheme that combines the invariant feature extraction with watermark embedding by using Tchebichef moments. Pham et al. [19] 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. Li et al. [20] presents two rotation invariant watermark embedding schemes in the nonsubsampled contourlet transform (NSCT) domain based on the scale-adapted local regions. 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, some researchers introduced the machine learning theory to image watermarking [21–24]. Khan et al. [25] presented an innovative scheme of blindly extracting message bits when a watermarked image is distorted. In this scheme, the authors exploited the capabilities of machine learning (ML) approaches for nonlinearly classifying the embedded bits. The proposed technique adaptively modifies the decoding strategy in view of the anticipated attack. The extraction of bits is considered as a binary classification problem. Usman et al. [26] proposed a novel approach of adaptive visual tuning of a watermark in discrete cosine transform (DCT) domain. The proposed approach intelligently selects appropriate frequency bands as well as optimal strength of alteration. Genetic programming (GP) is applied to structure the watermark by exploiting both the characteristics of human visual system and information pertaining to a cascade of conceivable attacks. The developed visual tuning expressions are dependent on frequency and luminance sensitivities, and contrast masking. To further enhance robustness, spread spectrum based watermarking and Bose–Chadhuri–Hocquenghem (BCH) coding is employed. The combination of spread spectrum sequence, BCH coding and GP based non-linear structuring makes it extremely difficult for an attacker to gain information about the secret knowledge of the watermarking system. Peng et al. [27] proposed a novel image watermarking method in multiwavelet domain based on support vector machines (SVMs), in which the special frequency band and property of image in multiwavelet domain are employed for the watermarking algorithm. Tsaia et al. [28] presented a robust lossless watermarking technique based on α-trimmed mean algorithm and support vector machine (SVM), in which the SVM is trained to memorize relationship between the watermark and the image-dependent watermark other than embedding watermark into the host image. Li et al. [29] introduced 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.

Through a large number of theory analysis 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 attacks, such as edge sharpening, histogram equilibrium, length-width ratio change, cropping, mixed attacks, etc., this mainly due to the poor feature vectors.
- 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 SVM and Gaussian–Hermite moments 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 adaptively the NSCT coefficients in small block. The main steps of digital watermark detecting procedure include: (1) some low-order Gaussian–Hermite moments of training image are computed, which are regarded as the effective feature vectors; (2) the appropriate kernel function is selected for training, and a SVM training model can be obtained; (3) the watermarked image is corrected with the well trained SVM model; (4) the digital watermark is extracted from the corrected watermarked image.

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

2. Support vector machine (SVM)

In this section, we briefly introduce the standard SVM for binary classification problems.

Support vector machines (SVM) have been successfully applied in classification and function estimation problems after their introduction by Vapnik within the context of statistical learning theory and structural risk minimization [30]. Vapnik constructed the standard SVM to separate training data into two classes. The goal of the SVM is to find the hyperplane that maximizes the minimum distance between any data point, as shown in Fig. 1.

For the training sets

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$$

$x \in R^n$, $y \in R$, to get the relation between the input x_i and output y_i, it can seek an optimal function $f(x)$ by SVM training, so that the difference between the output value and the corresponding objective value of every input samples is not more than error ε. For the linear situation, the form of function is: $f(x) = \omega \cdot x + b$, $\omega \in x$,